Signaux

Revue de L'Association des Diplômés de l'I.S.E.P.
Janvier 2013 - N°104

Le Management du Risque

isep Alumni

SOMMAIRE

Association des Diplômés de l'Institut Supérieur d'Électronique de Paris
28 rue Notre Dame des Champs - 75006 Paris - Tél. : 01 49 54 52 89
www.isepalumni.fr

Directeur de la Publication : Bruno de la Porte - Rédacteur en chef : Michèle Germain
Conception : DHTL

Editorial

Par Michèle Germain - ISEP 1968

Le risque est là, nous le côtoyons au quotidien, tant dans notre vie professionnelle que dans notre vie privée. Les Entreprises le côtoient, les Collectivités et les États également.

Dans ce nouveau numéro de Signaux, nous allons nous intéresser aux risques qui menacent notre société et qui viennent de partout : de la dangerosité des installations et des techniques, de la malveillance, particulièrement féconde dans le domaine de l'informatique, de ceux qui viennent de l'environnement et de la pollution ou encore du management, comme en témoignent les grandes affaires bancaires de ces dernières années.

Le risque ne doit pas être accepté comme une fatalité. Avant tout, il faut l'identifier afin de savoir le gérer. Une nouvelle science est née qui est celle de *l'intelligence des risques*. Le risque connu, nous devons apprendre à le gérer en mettant en place une rigoureuse politique de prévention.

Mais il faut aussi envisager l'impensable, l'accident que rien ne laissait présager et devant lequel il va falloir réagir et non s'incliner. Une méthodologie appropriée permet de gérer de telles situations et d'en tirer un enseignement pour le futur.

La gestion du risque passe par la protection de l'information. Celle-ci est le patrimoine de l'Entreprise, de la Collectivité, de l'État. Elle est stockée et gérée par des systèmes d'information qu'il faut impérativement protéger. A l'heure de l'Internet et des réseaux, cette précieuse information est de plus en plus délocalisée dans des serveurs souvent situés à l'étranger, hors de notre juridiction, et dans les mains de sous-traitants avec lesquels il faut strictement fixer la règle du jeu.

La gestion du risque dépasse le cadre strict de l'entreprise et s'étend au risque sociétal. Les entreprises produisent, certes, mais se doivent de le faire sans risque pour notre société et sans brûler par les deux bouts les ressources de la planète. Cette prise de conscience débouche tout naturellement sur le développement durable.

Enfin, le risque informatique est beaucoup évoqué. Les menaces sur les entreprises et sur les particuliers sont bien connues. Mais plus rarement évoquées sont les attaques contre les États qui, en bloquant leurs moyens de communication et de production, peuvent devenir une puissante arme de guerre, ou plus exactement, de cyberguerre.

Vous découvrirez tous ces aspects du risque et management du risque au fil des pages de cette nouvelle édition de Signaux, à laquelle ont participé les meilleurs experts, anciens élèves, intervenants et enseignants de l'ISEP. L'équipe rédactionnelle de Signaux remercie tout particulièrement Bernard Besson et Jean-Claude Possin, experts en Intelligence Économique, pour leur contribution.

Le mot du président

Par Bruno de la Porte - Président d'ISEP Alumni

Notre revue Signaux se devait d'aborder un thème d'actualité comme celui du risque. Le risque est en effet présent au quotidien et dans tous les métiers pratiqués par nos diplômés, qu'ils interviennent dans l'aéronautique, les télécoms, la finance ou au sein d'une société de services (pour n'en citer que certains). D'ailleurs, il conviendrait mieux de parler « des risques », ou pour être constructif (comme se le doit tout bon ingénieur) du « management du risque ».

Je suis vraiment très fier de pouvoir confier à votre lecture le contenu de cette revue. Cette dernière reflète la diversité des formations proposées par l'école (tant via le cursus d'ingénieur qu'avec les MSc ou la formation continue), tout autant que la richesse des parcours professionnels réalisés par les diplômés de l'ISEP.

Cela nous confirme, s'il en était besoin, que la formation d'ingénieur est avant tout une formation pour apprendre à apprendre, afin de rester toujours à l'écoute en éveil ou en veille sur les évolutions de la société : technologiques, sociologiques, physiques… Le plus grand risque n'est-il pas de croire que tout est sous contrôle ou de souhaiter que rien ne change ?

Mais, je ne vais pas entrer dans un débat philosophique sur la gestion du risque. Je ne peux que vous conseiller une lecture attentive des articles riches de ce n° 104 de notre revue Signaux, afin de mieux appréhender ce management du risque au quotidien et dans des situations autant professionnelles que personnelles.

Et je forme un vœu : que ces articles, dont une très forte majorité est rédigée par des Isépiens, incitent d'autres « écrivains en herbe » à oser prendre la plume afin de partager leur savoir et leur expérience. *Il n'est de richesses que d'hommes* disait Jean Bodin ! Alors profitons-en et partageons.

De la sécurité économique à l'intelligence des risques ?

Par Bernard Besson, dirigeant de Bernard Besson Consulting et Jean Claude Possin, INHES-J, Consultant

La sécurité économique est depuis longtemps un métier exercé par des professionnels reconnus[1]. Normalisée[2] à l'échelle mondiale à partir du 11 septembre 2001 et façonnée en France par la jurisprudence de la Cour de Cassation, elle est aujourd'hui un concept en voie de dépassement.

Il ne suffit plus en effet de s'assurer contre les risques. Il convient de les anticiper afin de les éviter et les transformer en avantages compétitifs. Les entreprises souhaitent une « intelligence des risques » sur mesure. Elles veulent un système à géométrie variable leur permettant d'ajuster leur sécurité économique à des budgets souvent en voie de réduction.

L'intelligence des risques est une application de l'intelligence économique au domaine de la protection. Elle inspire le quotidien des Risk managers qui voient dans cette nouvelle approche une adaptation à la crise et une extension de leur métier[3].

Avec l'intelligence des risques, l'entreprise appréhende, dans un même effort de compréhension et d'anticipation, des risques et des menaces qui étaient jusqu'alors traités séparément. Elle repère ainsi des interactions, des effets pervers, des risques interstitiels qui échappaient à sa vigilance.

Quatre familles de risques regroupent l'ensemble des aléas susceptibles d'altérer les performances de l'entreprise.

La sécurité *(safety)*, première famille, traite des risques et accidents involontaires liés aux technologies et aux installations classées dangereuses. Nous sommes ici dans le domaine de la sécurité industrielle, de l'incendie, de l'hygiène et de la sécurité, des accidents du travail ou du manque de précautions techniques.

La présence d'amiante dans un bâtiment ou de nitrate d'ammonium à l'usine AZF de Toulouse illustre ce qu'il convient d'entendre par *sécurité*. Très encadrée et bénéficiant de spécialistes hautement qualifiés cette famille de risques a été à l'origine de nombreuses études scientifiques. Elle a permis la mise en place d'une culture et d'un cadre conceptuel propices au traitement effectif de ces risques.

La sûreté *(security)*, seconde famille, traite des menaces liées aux malveillances humaines. Agressions physiques, racket, contrefaçon, intrusions dans les systèmes informatiques, fraudes, abus de biens sociaux, abus de confiance, escroqueries, trafic d'influence, détournements, vols, déstabilisation, terrorisme, piratages, espionnage, emprise sectaire constituent le champ de la *sûreté*. Les innombrables formes de la malveillance humaine relèvent du code pénal et du droit pénal spécial.

Leur ingéniosité, leur diversité, l'utilisation de vulnérabilités techniques liées à une parfaite maîtrise des technologies de l'information, plaident en faveur d'une intelligence globale de toutes les interactions possibles entre cette famille et les autres. Son appréhension au sein de l'entreprise, par

[1] Association des managers de l'assurance et du risque en entreprise (AMRAE), Club des directeurs de la sécurité d'entreprise (CDSE), Club de la sécurité de l'information français (Clusif) etc.

[2] ISO 280000, ISO 27000, ISO 31000 etc. Il n'existe pas en France de stratégie nationale alliant secteur privé et public capable de donner un contenu précis et exhaustif à la notion de « sécurité économique ». Ce sont les concepts anglo-saxons qui s'imposent à travers les processus de certification. Ces standards puisent d'ailleurs abondement dans le travail de nos ingénieurs et spécialistes des cindyniques. Ce paradoxe s'explique par l'absence d'État stratège dans un domaine qui est perçu ailleurs comme un domaine de souveraineté. Mais aussi un business mobilisant des entreprises comprenant des milliers, voire de dizaines de milliers de professionnels de la sécurité économique.

[3] Bernard Besson et Paul Vincent Valtat Le Risk manager et l'intelligence économique. 2008, éditions AMRAE

d'authentiques professionnels[1], est un exercice d'autant plus difficile que les formations de qualité dans ce domaine sont rares.

Les risques environnementaux, troisième famille, font l'objet d'une approche plus récente mais bien codifiée[2]. Il s'agit ici de prévenir les risques naturels liés aux inondations, aux incendies de forêt, aux tremblements de terre, mais aussi de prévenir les risques liés au traitement de l'eau, au traitement des déchets, aux odeurs, aux bruits, aux pollutions de l'air, des sols et des rivières, aux gaz à effet de serre, etc. Le droit des catastrophes naturelles et le concept de développement durable ont généré une véritable communauté d'acteurs et de spécialistes qui rendent incontournable la prise en compte de l'environnement.

Les risques managériaux relèvent d'une quatrième famille. Jusqu'à présent ils n'étaient pris en compte qu'occasionnellement dans l'entreprise notamment à l'occasion d'une gestion de crise. Leur adjonction systématique aux précédents constitue l'un des apports originaux de l'intelligence des risques. Leur nombre comme celui des autres menaces est illimité. Ceux cités dans cet article donnent une idée des vulnérabilités possibles :

- absence de système d'intelligence économique,
- absence de gestion anticipée de crises,
- absence de gestion de risques,
- absence de mission de protection,
- affaiblissement du processus de décision,
- amnésie des savoirs, savoir-faire et compétences,
- assurantiel (défaut de police et dissémination d'informations sensibles),
- cécité technologique,
- client (insolvabilité),
- concurrentiel,
- conjonction d'évènements,
- effets secondaires et pervers,
- entrepreneurial (premier de tous les risques),
- éthique, déontologique (absence de…),
- financier, actionnarial et boursier,
- image (affaiblissement et perte de réputation),
- informationnel (rumeurs, déstabilisation…),
- informatique (systèmes d'information inadaptés),
- juridique,
- stratégique (absence de vision),
- pays (risque pays),
- perte d'influence,
- perte d'opportunité,
- perte de compétitivité,
- produit,
- rupture d'approvisionnement,
- social,
- sociétal.

D'autres risques auraient pu y figurer comme le boycott, le risque de délocalisation, d'absence de reporting, le risque d'attentisme, de dépendance énergétique, de résistance au changement. Chaque entreprise établit sa propre liste des risques managériaux en fonction de ses craintes et de ses capacités d'anticipation.

Les risques de management naissent le plus souvent d'une absence de stratégie, d'une mauvaise gouvernance ou d'une confluence d'événements. Chacun peut faire l'objet d'une prévention particulière, mais une vision d'ensemble permettra de prévenir l'interaction d'un risque sur un autre.

Le regard global n'a d'ailleurs aucune raison de se limiter aux risques managériaux. C'est l'ensemble des risques des quatre familles que l'organisation doit observer.
Ce que nous appelons le *Risque Sécuritaire Global* (RSG)[3] suppose une veille globale.

Le RSG[4] est l'ensemble des risques recensés de Sécurité, de Sûreté, d'Environnement et de Management. Il se présente graphiquement soit sous forme de panorama, soit sous forme *d'histogramme*.

$$\mathbf{RSG = \sum R.\ Sécurité + \sum R.\ Sûreté + \sum R.\ Environnementaux + \sum R.\ Managériaux.}$$

Ce traitement global relève d'une décision stratégique prise au sommet de l'entreprise. Il s'agit d'associer dans un même système la *mission de protection* de l'organisation et la *gestion des risques* telle qu'elle est déjà pratiquée.

L'intelligence des risques[5] détaille le processus managérial et juridique qui permet d'associer les attributions du directeur de la gestion des risques et du délégué général à l'intelligence économique. Elle retrace les étapes qui au sein de l'entreprise débouchent sur la mise en œuvre d'une véritable mission de protection dotée d'un statut de direction à part entière.

[1] En dehors d'anciens policiers ou gendarmes rompus aux problèmes de délinquance et spécialisés dans le droit pénal spécial et la procédure pénale. Là encore l'entreprise qui recrute devra judicieusement choisir le profil retenu car tous ne sont pas en adéquation avec ses besoins. Une telle approche nécessite l'avis d'un bon spécialiste.
[2] ISO 14000
[3] Les termes risque sécuritaire global (RSG) et Intelligence des risques sont des titres déposés et protégés par l'éditeur.
[4] Le RSG d'une entreprise est une donnée qui correspond à la moyenne des criticités pondérées des risques retenus.
[5] Besson B, Possin J C L'Intelligence des risques, IFIE 2ème Edition janvier 2008.

En tant qu'outil de management de l'entreprise, l'intelligence économique apporte une nouvelle dimension à la gestion traditionnelle des risques.

Elle induit une économie d'échelle qui permet d'optimiser la recherche et le recueil des informations. Elle réduit les coûts de la protection[1] d'entreprise.

L'organisation décloisonne la lecture traditionnelle de toutes les menaces qui pèsent sur elle[2].

>>> RASSEMBLER LES COMPETENCES

Pour le système d'intelligence économique, chaque risque, quel qu'il soit, est avant tout *une information* que l'entreprise a ou n'a pas, qu'elle peut recueillir et analyser afin de décider et de prévenir.

La démarche d'intelligence économique rejoint ici la démarche habituelle des cindyniques[3].

Pour les sciences du danger, chaque incident, accident ou crise majeure s'analyse par des défauts dans le recueil, l'interprétation, la transmission et la prise en compte de l'information.

A cet égard, la catastrophe du tunnel sous le Mont Blanc ou la faillite commerciale d'une entreprise s'expliquent de manière identique. Un processus cognitif et décisionnel est interrompu. Des informations ont manqué ou n'ont pas été transmises. Transmises, elles n'ont pas été lues ou correctement interprétées. Analysées, elles n'ont pas été prises en compte.

Les gestionnaires et praticiens[4] du risque disent tous combien la maîtrise de l'information est le préalable incontournable de la gestion des risques. La similitude des approches entre gestion des risques et démarche d'intelligence économique fonde les concepts *d'intelligence des risques* et *de risque sécuritaire global*.

Les veilles coordonnées du système d'intelligence économique éclairent chaque risque tout en le comparant aux autres.

- Elles permettent d'identifier, de calculer et de hiérarchiser les risques à partir de leur fréquence, de leur gravité et de leur probabilité.
- Elles accompagnent leur prévention, leur réduction et leur éradication.

Le traitement commun et généralisé des risques de sécurité, de sûreté, environnementaux et managériaux se fonde sur une réalité parfois cruelle.

Le drame de la navette Columbia[5] illustre de manière spectaculaire l'interférence des risques de sécurité et de management. Selon le Columbia Accident Investigation Board (CAIB), les spécialistes de la gestion des risques de la NASA avaient depuis longtemps signalé les risques inhérents à la chute d'isolants provenant du réservoir externe sur les ailes de la navette.

A huit reprises, des informations orales et écrites permettant de prendre conscience de la fréquence et de la gravité de ce risque ont été négligées.

Ce sont, au dire de l'enquête, les cloisonnements entre les différents métiers, entre les certitudes des uns et des autres, entre les sources d'information qui ont tué les sept astronautes.

Beaucoup plus que la détérioration du bouclier thermique, c'est la conjonction des risques de sécurité et de management qui a été à l'origine du drame. L'absence de vision globale explique beaucoup de catastrophes.

Les conséquences du tsunami du 26 décembre 2004 trouvent une partie de leur explication dans la conjonction de risques environnementaux (région à forte activité sismiques), managériaux (défaut de systèmes d'alerte), de sécurité (édifices sans normes parasismiques) et de sûreté (corruption des maîtres d'ouvrage).

De façon moins spectaculaire mais tout aussi vraie, la baisse de performance d'une entreprise s'explique souvent par la convergence de risques provenant de plusieurs familles :

L'entreprise est victime d'un risque de taux de change sur

---

[1] *Au sens général et habituel, la sécurité est l'aptitude des organisations à prévenir la survenance d'événements graves, critiques ou catastrophiques. Elle concerne les personnes et les biens matériels et immatériels.*

[2] *Référentiel de formation en intelligence économique rédigé par la Commission Consultative Nationale réunie à l'initiative du Haut Responsable pour l'Intelligence Économique auprès du Premier Ministre, et présenté au public le 23 mai 2005. L'Intelligence des risques s'inscrit dans la philosophie générale de ce document et notamment des pôles 3 et 4 respectivement intitulés : Management de l'information et des connaissances. Protection et défense du patrimoine informationnel et des connaissances.*

[3] *Georges Yves Kerven Eléments fondamentaux des cindyniques Economica 1995. Les dangers font l'objet d'une science qui s'appelle les «cindyniques», du grec kindunos qui signifie danger.*

[4] *Geiben B, Nasset J J Sécurité, Sûreté, la gestion intégrée des risques dans les organisations. Éditions d'organisation 1997.*
Roux-Dufort Ch., Gérer et décider en situation de crise, outils de diagnostic, de prévention et de décision. Dunod, 2ème édition 2003.

[5] *« Le Monde », 28 août 2003 ; page 2 La NASA sévèrement mise en cause dans le drame de Columbia.*

une devise étrangère (risque managérial), d'une panne de son système d'information (risque de sécurité), d'un vol de données informatiques (risque de sûreté), d'une pollution des eaux (risque environnemental).

La variété, l'interaction et l'évolution permanente des risques et menaces interdit malheureusement toute solution définitive. Le risque zéro n'existe pas et aucune gestion des risques ne mettra l'entreprise à l'abri d'une crise.

L'imprévisibilité demeure un facteur incontournable, même si la prise en compte d'informations validées et l'élaboration de scénarii catastrophe en limite l'occurrence et l'amplitude.

L'intelligence des risques n'est pas la boule de cristal qui permet de prévoir chaque accident ou incident. Elle est un système transversal et collectif, une perception sensorielle qui permet de capter et d'interpréter des signaux faibles, des indices émergents comme des tendances lourdes.

Le risque est à la fois endogène et exogène, interactif et polymorphe. Sa prévention ne peut relever que de l'intelligence collective de ses victimes potentielles. Il existe une manière, de réfléchir, d'anticiper ensemble.

Chaque risque ou menace s'assimile à une communauté de personnes appartenant au dedans et au dehors de l'entreprise. Le risque devient un réseau de connivence et d'échanges rassemblant des spécialistes, des témoins, des victimes.

Ces réseaux sont par principe inachevés et illimités. Le risque, ainsi commenté et analysé, alimente une mémoire spécifique, elle aussi inachevée et située à la fois au-dedans et au dehors de l'entreprise.

Chaque menace devient ainsi une économie de transactions de données et d'alertes qui alimentent une base de données décisionnelles.

Le risque incendie d'une entreprise industrielle rassemble dans une même communauté des personnes aussi variées que le technicien de la sécurité incendie, les services de secours de la commune, les services de la sécurité civile, la police, la médecine du travail, l'inspection du travail, le service de gardiennage, les experts et consultants en sécurité incendie, les assureurs, le service de la voirie de la municipalité, les entreprises sous-traitantes, l'inspection départementale des installations classées, le comité d'hygiène et de sécurité, le comité local de prévention des risques industriels, la veille juridique de l'entreprise, la veille normative de la branche professionnelle à laquelle appartient l'entreprise, etc.

La gestion des risques relève de l'animation et de la coordination de ces communautés. Cette animation repose essentiellement sur la circulation de questions et de réponses, sur la fabrication de connaissances inédites débouchant sur des prises de décisions.

L'entreprise se protège en fusionnant la gestion traditionnelle des risques et le système d'intelligence économique. Si celui-ci n'existe pas encore, la mission de protection se dotera de son propre système d'information de gestion des risques (SIGR)[1].

Les audits de sécurité/sûreté montrent que l'entreprise vient la plupart du temps à l'intelligence économique par le biais d'un accident ou d'une catastrophe. C'est cette réalité constatée par les auteurs sur le terrain qui les a conduits à fusionner les deux approches dans un même ouvrage.

Pour être crédible, la sécurité doit devenir une sécurité partagée par le plus grand nombre d'acteurs permanents ou occasionnels. Cette multiplication des perceptions et des interprétations implique une coordination et une centralisation à des fins de d'évaluation et de hiérarchisation.

Risques et menaces sont réduits à partir du moment où ils sont nommés et calculés. Un risque dont on parle est un risque en partie maîtrisé.

L'intelligence des risques est un langage transversal qui permet aux différentes directions et unités de l'entreprise de communiquer entre elles et avec l'extérieur. Ce langage est transposable dans le domaine public et permet de bâtir l'intelligence des risques d'un territoire, d'une agglomération de communes ou d'une branche professionnelle.

>>> HIERARCHISER LES RISQUES DANS UN PANORAMA D'ENSEMBLE

Le directeur de la gestion des risques doit fournir à l'organisation un panorama complet et hiérarchisé de tous les risques et menaces qui la concerne.

Ces risques seront périodiquement revisités, remis à jour et comparés les uns aux autres en fonction de leur *criticité pondérée*.

[1] *Ce que préconisent les gestionnaires de risques « Fonction : Risk manager » de Catherine Véret et Richard Mekouar. Dunod janvier 2005*

La criticité pondérée d'un risque se calcule selon une formule mathématique simple[2] que nous proposent MM. Geiben et Nasset dans le domaine de la sécurité. Il nous paraît possible et souhaitable d'étendre ce mode de calcul à l'ensemble des risques et des menaces.

La criticité d'un risque est égale à sa fréquence que multiplie sa gravité.

Criticité = Fréquence (F) x Gravité (G)

Fréquence et gravité n'ont pas la même signification selon les secteurs ou les branches professionnelles. Un défaut de fabrication dans l'industrie aéronautique n'a pas la même gravité qu'un défaut de fabrication dans le domaine de la pâte à papier. La fréquence des accidents n'a pas la même portée dans le domaine hospitalier que dans le domaine agricole.

Chaque entreprise et chaque communauté de risque participe à l'élaboration de coefficients de pondération de la fréquence (Fp) et de la gravité (Gp) qui tiendront compte du chiffre d'affaire, des normes d'une profession, des réactions de la clientèle, de la culture de l'entreprise et de son environnement économique.

La criticité pondérée d'un risque sera dès lors égale à sa fréquence pondérée multipliée par sa gravité pondérée.

Cp = Fp x Gp

L'intelligence des risques offre sans prétention scientifique un langage commun aux acteurs internes et externes de la prévention. Ce langage, ces sujets de conversation, voire de polémiques, seront le ciment d'une véritable protection fondée sur le partage des informations.

[1] *Geiben B, Nasset JJ ; ouvrage déjà cité.*

>>> A PROPOS DES AUTEURS

Ancien élève de l'École supérieure de police de Saint Cyr au Mont d'Or d'où il est sorti avec le grade de commissaire de police, aujourd'hui Contrôleur Général de la Police Nationale, **Bernard Besson** a été depuis 1976 successivement chef du service des renseignements généraux de Roanne, adjoint au directeur de renseignements généraux de Lyon, directeur départemental des renseignements généraux de la Nièvre, directeur de cabinet du Directeur Central des Renseignements Généraux puis du Directeur de la Surveillance du Territoire (DST). Après avoir été membre de l'Inspection Générale de la Police Nationale, il a dirigé la police des Courses et des Jeux au Ministère de l'Intérieur de 1998 à 2004. Affecté par le Ministre de l'Intérieur en 2004 auprès du Haut responsable à l'intelligence économique, il s'occupe des dossiers Formations, Métiers de l'intelligence économique et PME. A ce titre il préside les groupes de travail « Formation » et « Métiers et compétences de l'intelligence économique ».

Conseil en Intelligence économique et management des risques, ancien auditeur de l'IHESI, créateur du cabinet SIES Consultants, **Jean-Claude Possin** est actuellement membre et ancien vice-président du Groupe Intelligence Économique (GIE) de l'Institut National des Hautes Études de la Sécurité (INHES-J). Il participe à des conférences, formations et colloques IEMA Alger et enseigne *l'Intelligence économique* et *l'Intelligence des risques* dans différents mastères : École Européenne d'Intelligence Économique (EEIE) Versailles, ISC Paris, CERAM Sophia Antipolis puis Skéma Business School Pôle Universitaire Léonard de Vinci Paris, ESIEE, Institut Supérieur d'Électronique de Paris (ISEP), formations à l'IFIE, etc. Il est co-auteur avec B. Besson de plusieurs ouvrages sur l'Intelligence économique.

Jean-Claude Possin et Bernard Besson signent la rubrique « Méthodologie et bonnes pratiques » de Regards sur l'IE, ainsi que de nombreux articles dans Veille Magazine et autres publications.

Sécurité de l'information

Par Patrice KAHN
ISEP 1981
Gérant – Fondateur de la société KSdF-Conseil

>>> L'INFORMATION : UN BIEN A PROTEGER

L'information se présente sous trois formes : les données, les connaissances et les messages. On a l'habitude de désigner par « système d'information » l'ensemble des moyens techniques et humains qui permet de stocker, de traiter ou de transmettre l'information.

Le concept de sécurité des systèmes d'information recouvre un ensemble de méthodes, techniques et d'outils chargés de protéger les ressources d'un système d'information afin d'assurer :

- **la disponibilité des services :** les services (ordinateurs, réseaux, périphériques, applications…) et les informations (données, fichiers…) doivent être accessibles aux personnes autorisées quand elles en ont besoin ;
- **la confidentialité des informations :** les informations n'appartiennent pas à tout le monde ; seuls peuvent y accéder ceux qui en ont le droit ;
- **l'intégrité des systèmes :** les services et les informations (fichiers, messages…) ne peuvent être modifiés que par les personnes autorisées (administrateurs, propriétaires…).

La « politique de sécurité » d'une entité (société, organisme public, unité d'enseignement ou de recherche, …) est l'expression de ces objectifs. Elle doit indiquer l'ensemble des mesures à prendre, des structures à définir et l'organisation à mettre en place, afin :

- d'empêcher (ou tout au moins freiner) la détérioration, l'utilisation anormale ou la pénétration des systèmes et réseaux ;
- de détecter toute atteinte, malveillante ou non, à l'intégrité, la disponibilité et la confidentialité des informations ;
- d'intervenir afin d'en limiter les conséquences et, le cas échéant, poursuivre l'auteur du délit.

On ne protège bien que ce à quoi on tient, c'est-à-dire ce à quoi on associe « une valeur ». La trilogie confidentialité, intégrité, disponibilité, détermine la valeur d'une information. La sécurité des systèmes d'information (SSI) a pour but de garantir la valeur des informations qu'on utilise. Si cette garantie n'est plus assurée, on dira que le système d'information a été altéré. Une altération n'est pas uniquement le fait de malveillances. Il est plus souvent encore, la conséquence de pannes, de maladresses, d'accidents ou d'erreurs humaines dont les plus fréquentes sont les erreurs de conception. Ces phénomènes relèvent de la « sûreté de fonctionnement » qui est une autre manière d'appréhender la sécurité globale. Les sauvegardes, le fonctionnement en mode de repli, la redondance, etc. font aussi partie de la trousse à outils traditionnelle de la sécurité prise dans son sens général.

Avec le développement de l'informatisation des échanges (courriers officiels, transactions financières, commerciales…), la simple affirmation de la valeur de l'information n'est plus suffisante. Il est nécessaire d'y adjoindre des propriétés nouvelles comme l'authentification (garantie de l'origine d'un message, de l'auteur d'un document), la paternité (l'information ne peut pas être répudiée par son auteur), la traçabilité (on connait le circuit qu'a suivi une information), etc. La préservation et la garantie de ces propriétés relèvent également de la fonction « sécurité ».

>>> LES SYSTEMES D'INFORMATION : UN OUTIL VULNERABLE

Les sources de dysfonctionnement des systèmes d'information sont diverses et variées. Elles ont le plus souvent des causes d'origine « humaines » :

- Les sauvegardes sont mal faites ou mal gérées et rendent le système sensible aux pannes, aux maladresses et aux sinistres ;
- L'absence d'une vision globale de la sécurité, traitée par petits morceaux, au cas par cas débouche immanquablement sur un manque d'organisation (qui fait quoi dans quelle structure ?) et plus spécialement sur de mauvaises architectures réseaux ;
- Le manque de consignes claires qui permettraient à chacun de savoir ce qu'il a à faire, ce qu'il peut faire et ce qu'il n'a pas le droit de faire ;

- La divulgation malencontreuse d'informations due à une imprudence ou un manque de vigilance ou une non-sensibilisation aux risques, ceci se traduisant par le non-respect de règles parfois élémentaires ou simplement d'un manque de conscience.

L'importance de l'information dans notre société s'est accrue dans les dernières décennies, en même temps que les moyens utilisables pour la création et l'échange d'information et en même temps, aussi, que les vulnérabilités des systèmes associés. Ce qui était compliqué est devenu complexe.

Quand les échanges étaient limités à des moyens de télécoms restreints, les risques étaient faibles tout comme le volume des informations que l'on pouvait échanger.

Avec l'ouverture des réseaux et le nouvel environnement créé par l'Internet, des millions d'individus aux motivations très différentes sont mis en relation de manière voulue ou non.

Du temps où l'informatique était centralisée, les menaces « physiques » (pénétration dans des locaux informatiques sans autorisation, vol, vandalisme…) représentaient les menaces majeures. En ces temps bénis, la protection pouvait se résumer en quelques mesures de contrôle d'accès : grosses serrures, sas et gardiens étaient la panoplie usuelle. La situation est aujourd'hui bien différente. Certes, il y a toujours les vols de matériel, l'utilisation de la console maîtresse pour pénétrer un système ou le piégeage d'un réseau Ethernet ou public pour le mettre sur écoute, mais globalement, la dangerosité de ce type de menaces, dont les remèdes sont connus et éprouvés, est sans commune mesure avec les agressions menées via le réseau, qui se réalisent sans la présence physique de l'agresseur. Ces agressions par le réseau ont maintenant très largement atteint un seuil critique et on ne sait pas toujours quelle parade leur opposer. Dans le palmarès de cette nouvelle délinquance, on retrouve pêle-mêle :

- Tout ce qui porte atteinte à l'intégrité du système :
  - le piégeage de systèmes (bombes logiques, chevaux de Troie, sniffeurs…) afin de nuire à l'entité ou de se donner les moyens de revenir plus tard.,
  - la modification des informations afin de porter atteinte à l'image de l'entité (exemple : modification de ses pages web),
  - l'utilisation des ressources du site visé,
  - une intrusion en vue « d'attaques par rebond », c'est-à-dire qu'une autre cible est visée, votre système servant seulement de point de passage. L'entité est alors complice involontaire du piratage.
- Tout ce qui porte atteinte à la confidentialité des informations :
  - la récupération d'informations sensibles (mots de passe, informations avant publication officielle, données personnelles, etc.),
  - la fouille des messages, des données, des répertoires, des ressources réseaux…
  - l'usurpation d'identité.
- Tout ce qui porte atteinte à la disponibilité des services :
  - la paralysie du système (considérée ensuite comme un exploit par les pirates qui l'ont réalisée),
  - la saturation d'une ressource (serveur, imprimante…),
  - les virus et vers informatiques.

>>> LES SYSTEMES D'INFORMATION : QUELLES PARADES ?

La Sécurité des Systèmes d'Information (SSI) repose sur l'utilisation de techniques comme l'authentification des utilisateurs, le contrôle d'accès aux ressources, la non-répudiation, l'audit des traces de sécurité, etc. Le niveau de sécurité globale d'un système est celui de son maillon le plus faible, aussi recherchera-t-on à élever le niveau de sécurité d'une manière homogène. Pour ne citer qu'un exemple : rien ne sert de rechercher la performance sur le plan technique en laissant pour compte les problèmes d'organisation ou de gestion des ressources humaines. La vérification de la cohérence de sécurité des systèmes se fait par une approche de type ISO 27000 (analogie des principes de l'ISO 9000 ou de l'ISO 14000 à la problématique de la SSI).

La SSI doit aussi prendre en compte la protection de la sphère privée, classe fonctionnelle des Critères communs (ISO 15408) déclinée en quatre propriétés : Anonymat, Pseudonymité, Non-chaînabilité, Non-observabilité.

La SSI ne se limite pas aux seuls aspects techniques. La réflexion doit se faire sur chacun des trois niveaux, stratégique, organisationnel et technique.

Un Système d'Information (SI) ne se maintient pas dans un état stable de sécurité. Il dérive de lui-même vers un état sans sécurité qui est son état naturel d'équilibre. Le maintien du niveau de sécurité se réalise par le pilotage de la politique de sécurité.

Le pilotage de la politique de sécurité s'appuie sur l'évaluation des écarts entre le niveau réel de sécurité et le niveau désiré. Les tableaux de bord sont des ensembles d'indicateurs définis à partir de la politique de sécurité et mis en forme afin de faciliter la perception de ces écarts au niveau technique, organisationnel et stratégique. Sans

politique de sécurité, la réalisation de tableau de bord n'a aucun sens. La politique de sécurité est corrigée suivant le cycle Prévention - Détection - Réponses.

Pour se prémunir contre une utilisation des réseaux qui viserait à s'approprier indûment des informations, il est nécessaire d'appliquer strictement quelques recommandations qu'il n'est pas inutile de rappeler :

- Adopter une architecture du réseau apte à interdire, ou tout au moins compliquer, toute tentative frauduleuse de pénétration ;
- Assurer une surveillance permanente des connexions extérieures afin de détecter au plus tôt tout accès anormal :
- Gérer rigoureusement les logins et les mots de passe en veillant plus particulièrement à n'accorder aux personnels non permanents (intérimaires, stagiaires, ...) que les facilités strictement indispensables à leurs travaux et à les leur retirer dès la fin de leur présence ;
- Imposer des précautions supplémentaires aux personnels ayant à se connecter de l'extérieur (et a fortiori lors d'un séjour à l'étranger), par exemple l'emploi de mots de passe à usage unique ;
- Utiliser, en cas de nécessité, les nouveaux procédés de chiffrement pour assurer la discrétion des échanges de messagerie et de données ;
- N'effectuer les travaux les plus sensibles et ne stocker les fichiers confidentiels que sur des machines physiquement déconnectées du réseau.

Mais les systèmes informatiques ne sont pas vulnérables qu'aux attaques extérieures.

L'incendie, l'explosion ou le dégât des eaux, l'insouciance, la maladresse ou la malveillance d'un collègue, peuvent perturber gravement le fonctionnement de cet incomparable outil de travail et de communication. Il faut donc, outre les mesures détaillées plus haut, sauvegarder en un lieu sûr et distant les informations et les données que l'unité ne peut se permettre de perdre.

Il appartient à chaque responsable de services ou de département d'une entité de définir et mettre en œuvre la politique de sécurité de son unité, d'inciter chacun de ses collaborateurs à en prendre conscience et à s'y impliquer.

>>> LES NORMES ISO 27000 : UNE PARADE ORGANISATIONNELLE ET TECHNIQUE

La série des normes ISO 27000 a été spécialement réservée par l'ISO pour le domaine de la sécurité de l'information et plus particulièrement des Systèmes de Management de la Sécurité de l'Information (SMSI). Elle est naturellement en cohérence avec de nombreux autres domaines de normalisation incluant l'ISO 9000 (management de la qualité) et l'ISO 14000 (management environnemental).

Dans cette série ISO 27000 ont été publiés différents documents et normes, dont nombre d'entre eux sont maintenant bien connus. D'autres sont encore en préparation.

- ISO/CEI 27000 : Introduction et vue globale de la série de normes, et glossaire des termes communs ;
- ISO/CEI 27001 : Norme de certification des SMSI ;
- ISO/CEI 27002 : Guide des bonnes pratiques en SMSI (précédemment connu sous le nom de ISO/CEI 17799, et avant BS 7799 Partie 1) ;
- ISO/CEI 27003 : Guide d'implémentation d'un SMSI, lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information ;
- ISO/CEI 27004 : Norme de mesures de management de la sécurité de l'information ;
- ISO/CEI 27005 : Norme de gestion de risques liés à la sécurité de l'information ;
- ISO/CEI 27006 : Guide de processus de certification et d'enregistrement ;
- ISO/CEI 27007 : Guide directeur pour l'audit des SMSI ;
- ISO/CEI 27008 : Lignes directrices de vérification en matière de mesures de sécurité ;
- ISO/CEI 27011 : Guide pour l'implémentation de ISO/CEI 27002 dans l'industrie des télécommunications ;
- ISO/CEI 27799 : Guide pour l'implémentation de ISO/CEI 27002 dans l'industrie de la santé.

A l'origine de cette série de ces normes reconnues est la norme ISO 17999 (maintenant ISO 27002) qui constitue le code de bonne pratique pour la gestion de la sécurité de l'information. Elle constitue un référentiel de bonnes pratiques de sécurité et des contrôles liés à leurs applications.

Cette norme est destinée aux dirigeants, aux directeurs de système d'information et aux responsables sécurité, notamment au RSSI (Responsable Sécurité des Systèmes d'Information), la personne qui a la responsabilité opérationnelle d'appliquer les règles à l'ensemble du domaine informatique. Il dispose du savoir-faire d'architecte technique de la sécurité et d'une parfaite connaissance des processus associés aux SI. La norme a été définie afin de répondre au besoin d'un « label de confiance » d'un organisme reconnu internationalement. Tout comme la norme

ISO 9000, la norme 27002 a pour objectif d'établir un label de confiance reconnu de tous en ce qui concerne la sécurisation de l'information sous un aspect global.

Les échanges de données nationales et internationales entre collaborateurs d'une même organisation, partenaires et clients couplés aux TIC, impliquent la nécessité de s'accorder sur une norme pouvant aider à sécuriser l'information et les processus d'échanges. La norme ISO 27002 propose un ensemble de mesures organisationnelles et techniques, mais n'impose pas de solution technologique particulière.

Cette norme accorde une importance particulière à certains aspects cruciaux de la sécurité :

- le support des dirigeants quant à la mise en œuvre d'une politique de sécurité et la détermination des moyens humains à y associer,
- l'identification des menaces propres à l'organisation et l'évaluation des risques associés,
- la classification des informations afin de ne déployer les moyens que sur celles qui le nécessitent,
- les dispositions à mettre en œuvre afin d'instaurer une « culture sécurité ».

Le groupe dédié à la sécurité de l'information au sein de l'organisme ISO a aussi publié différents rapports liés à la SSI. Certains de ces rapports ne possèdent pas le statut de norme internationale, mais plutôt de guide technique, et peuvent apporter des informations complémentaires :

- ISO 13335 :
  - concepts et modèles pour la gestion de la sécurité des TIC,
  - techniques pour la gestion des risques relatifs à la sécurité des TIC,
  - techniques pour la gestion de sécurité IT,
  - sélection de sauvegarde,
  - guide pour la gestion de sécurité du réseau ;
- ISO 14516 : lignes directrices pour l'utilisation et la gestion des services de tiers de confiance ;
- ISO 15408 : critères d'évaluation de la sécurité des TIC ;
- ISO 18044 : gestion d'incidents de sécurité de l'information.

>>> CONCLUSION

La sécurité dépend de tous, et tous les facteurs interagissent entre eux. La qualité des hommes – compétence, motivation, formation – est importante ; il faut y porter un effort constant. Les techniques et les moyens financiers sont vitaux et ne doivent pas être négligés. Mais de tous les facteurs et acteurs qui interviennent dans les SI et contribuent à la force ou à la faiblesse de l'ensemble, les directeurs d'unité jouent le rôle essentiel. La SSI est une fonction de Direction. Cela ne veut pas dire que les directeurs doivent mettre une casquette et contrôler les identités. Cela signifie simplement qu'ils mettent en place une organisation et ont un style de direction qui favorise ou non la prise en charge de cette question, que ce sont eux qui déterminent la politique de sécurité de leur entité, et que ce sont eux qui la font appliquer.

Il n'y a qu'eux qui puissent le faire et rien ne se fera s'ils ne sont pas personnellement convaincus de l'importance de cette tâche.

De même, à l'autre bout de la chaîne, l'utilisateur final a la charge de l'exécution de tous les actes élémentaires de sécurité. S'il ne voit ces mesures que comme une somme de contraintes mises en place pour lui gâcher la vie, la partie est perdue d'avance. D'où l'importance des recommandations de sécurité et des chartes informatiques qui, accompagnées des explications nécessaires, sont avant tout un moyen de sensibilisation. Bien présentées, elles deviennent le « règlement intérieur du club des utilisateurs ». Elles sont alors facilement acceptées et la vie collective y gagne en qualité.

Image symétrique du laxisme, le rigorisme est une autre déviance des conceptions de la sécurité. Opposé en apparence, cet autre excès aboutit au même résultat : le blocage du SI. Il faut donc rappeler que la sécurité n'est pas une fin en soi. Il ne s'agit pas de partir à la quête de l'absolu ou de construire une nouvelle ligne Maginot réputée infranchissable, mais de déterminer un seuil de vulnérabilité acceptable en fonction de contraintes et d'objectifs, et d'en contrôler les défaillances par des alarmes, des audits, l'enregistrement des accès réseau.

Enfin, il existe une autre manière de nier la sécurité : appliquer des règles toutes faites, sans les comprendre et sans considération des circonstances. La politique de sécurité doit respecter les spécificités fortes qui caractérisent notre milieu, faute de quoi elle subirait inévitablement un rejet. Ces spécificités sont principalement l'ouverture, l'imbrication des structures et le modèle organisationnel.

Les systèmes informatiques et les réseaux, qui étaient naguère l'outil d'une certaine élite, sont maintenant au cœur de tous les systèmes. Ce développement technique a permis d'accroître considérablement nos capacités de traitement, de stockage et de transmission de l'information, mais il a rendu en même temps les SI beaucoup plus fragiles. La gravité des accidents, des maladresses, des erreurs ou des malveillances est bien plus grande qu'auparavant : c'est

souvent la perte de plusieurs jours, parfois de plusieurs semaines de travail. Ces pertes peuvent être même irréparables. Parallèlement, les techniques et les savoir-faire se sont généralisés.

Il y a vingt ans, attaquer un système informatique centralisé demandait une certaine « technicité » qu'il n'est plus nécessaire de posséder aujourd'hui. On trouve sur Internet les « boîtes à outils » toutes prêtes qui permettent d'attaquer n'importe quel site, surtout s'il est mal administré.

Même Internet a changé. A l'origine, c'était un réseau limité à des personnes d'une même communauté scientifique. Les malveillances étaient rares car il était facile de connaître l'identité d'un interlocuteur.

Maintenant l'Internet est un réseau ouvert et anonyme que certains voudraient transformer en zone de non-droit. Nos habitudes d'utilisation des services de ce « réseau planétaire », ainsi que l'organisation de nos systèmes d'informations qui datent de cette époque révolue, doivent changer eux aussi. Cela prendra du temps car la tâche est immense.
Raison de plus pour commencer maintenant.

>>> POUR ALLER PLUS LOIN :

- Clusif : Club de la Sécurité de l'Information Français. www.clusif.fr
- CNRS ; Sécurité des systèmes d'information – Principes et enjeux. www.dgdr.cnrs.fr/FSD/securite-systemes/principes et enjeux.htm
- Normes ISO 27000 : http://www.iso.org

>>> ANNEXE – EXEMPLE DE CONTENU D'UNE POLITIQUE DE SECURITE

Afin de développer une politique de sécurité de l'information, il faut s'appuyer sur des normes et méthodes. Cette tâche est généralement la première mission qu'un RSSI doit réaliser en s'appuyant sur des normes et méthodes reconnues.

Les politiques de sécurité dérivées de normes reconnues, se déclinent en fonction de deux échelles de recommandations :

- Light Information Security Policy : une politique de sécurité de l'information modeste,
- Reinforced Information Security Policy : une politique de sécurité de l'information renforcée.

La liste des recommandations présentées ci-après s'applique à une politique renforcée. L'identification des recommandations pour une politique modeste peut être faite en éliminant certaines recommandations jugées trop lourdes ou non applicables au sein de l'organisation concernée.

MATERIEL, PERIPHERIQUES ET EQUIPEMENT DIVERS

- Fournir une alimentation électrique continue aux équipements critiques (UPS).
- Prévoir une génératrice de courant comme relais aux UPS.
- Limiter l'utilisation du fax (appareil ou modem) afin de réduire la potentialité de fuite d'information.
- Utiliser des modems PSTN/ISDN ou des lignes DSL avec précaution : toute transmission d'information critique ou confidentielle via ces systèmes de communication doit être réfléchie si aucun outil de protection (cryptographie) n'est utilisé.
- Contrôler l'utilisation des outils d'impression (imprimante locale, imprimante réseau, etc.). Aucune information critique ou confidentielle ne doit être imprimée sans avoir l'assurance que la transmission n'est pas sécurisée. De plus, l'utilisation de ressources d'impression distante doit prendre en compte le fait qu'un individu non autorisé peut potentiellement s'emparer des documents imprimés.
- Contrôler l'infrastructure d'interconnexion informatique (câblage réseau). Toutes les portes d'accès au réseau doivent être identifiées et chaque porte non utilisée doit être formellement identifiée, voire même déconnectée.
- Supprimer les données sur les matériels obsolètes qui ne sont plus utilisés.
- Verrouiller chaque station de travail (par exemple via un écran de veille avec verrou) lorsque son utilisateur n'est pas à son poste. Les mesures nécessaires (par exemple un verrouillage automatique après une certaine période d'inactivité) seront mises en place afin de pallier un éventuel manquement de l'utilisateur. Toute station serveur doit impérativement être verrouillée lorsqu'aucun responsable de sa gestion ne l'utilise.
- Vérifier lors de la mise en place d'un Intranet/Extranet qu'aucune porte dérobée n'a été ouverte. En effet, une telle faille permettrait le contournement des systèmes d'identification mis en place.

TRAVAIL EN DEHORS DE LOCAUX DE L'ORGANISATION ET UTILISATION DE PERSONNEL EXTERNE

- Définir correctement le cadre associé à la mission d'un prestataire de services informatiques externe. Un « Service Level Agreement » doit définir les rôles, droits et obligations auxquels le prestataire de service doit se

conformer pour garantir le bon fonctionnement des tâches qui lui sont confiées, ainsi que la confidentialité des informations qu'il pourrait être amené à manipuler.

- Contrôler l'attribution d'ordinateurs portables au personnel. L'utilisation de cet ordinateur portable doit être restreinte aux seules applications autorisées dans le cadre de la fonction professionnelle. Pour ce faire, une administration système robuste devra être mise en œuvre sur le système informatique portable afin de garantir que la règle ne puisse être contournée. Finalement, les mesures nécessaires (cryptage du disque local, droits utilisateur restreints, système d'authentification forte, etc.) devront être mises en œuvre afin d'assurer la confidentialité de l'information pouvant être disponible en cas de perte ou de vol de l'équipement mobile.
- Contrôler l'accès distant par le personnel (VPN, télétravail, etc.) aux ressources informatiques. Les mesures nécessaires (droits utilisateur restreints, système d'authentification forte, filtrage du trafic réseau non opportun, etc.) devront être mises en œuvre afin d'assurer une protection complète de l'antenne distante de l'organisation.

CONTROLE DE L'ACCES AUX SYSTEMES D'INFORMATION ET AUX CONTENUS QUI Y SONT PRESENTS

- Mettre en place une méthode d'authentification uniforme, maîtrisée et gérée de manière centralisée. De plus, il est conseillé de pouvoir utiliser cette même infrastructure d'authentification avec les différents systèmes nécessitant une identification d'utilisateur.
- Classifier chaque information mise à disposition sur l'infrastructure informatique et l'associer à des profils d'utilisation. Chaque profil identifié sera doté d'un ensemble de droits d'accès lui permettant l'usage des informations qui lui sont liées. De plus, les informations identifiées comme critiques ou confidentielles feront l'objet de mesures particulières assurant la sécurité nécessaire (cryptage de certains contenus sur leur support de stockage et lors de leur transfert sur le réseau de communication, introduction d'un système d'audit de consultation, etc.).
- Associer l'accès aux ressources réseau (imprimante, scanner, unité de stockage, Internet, etc.) à un mécanisme d'identification et d'audit. Le matériel nécessaire aux ressources réseau sera en outre protégé contre des accès en mode direct, c'est-à-dire sans passer par le système de contrôle d'accès (file d'impression sur serveur obligatoire, proxy pour Internet, etc.).
- Réserver les droits « administrateur » aux membres du groupe d'administration informatique. Tous les postes de travail doivent être administrés de telle sorte qu'aucune opportunité d'obtention de tels droits système ne soit possible par du personnel non autorisé. Ceci inclut l'impossibilité pour un utilisateur de modifier (ajout/suppression de programme) la configuration et la stabilité de son poste de travail. De plus chaque poste de travail ne comportera que les applications indispensables à la réalisation des tâches associées à la fonction de l'utilisateur de ce poste.
- Définir une politique de sélection de mot de passe pour les comptes informatiques. Aucun compte générique ne pourra être associé à un groupe d'utilisateurs ayant la même fonction. Les mots de passe vides ne sont pas tolérés et la durée de validité sera déterminée, avec un système de renouvellement forcé. Pour le groupe d'administration informatique, chaque responsable aura son propre compte associé aux droits d'administrateur système et toutes les actions d'administration seront réalisées sous l'identité effective du responsable. De plus, un système d'audit sera mis en place pour permettre la traçabilité des actions réalisées.
- Placer les systèmes informatiques sensibles (serveurs, routeurs, commutateurs, etc.) dans des locaux à accès restreint. L'accès physique à ces locaux sera limité au personnel autorisé. Le local sera fermé et un mécanisme d'identification (badge électronique, code personnel, etc.) sera mis en place, de même qu'un système d'audit, si cela est possible. Une attention particulière sera accordée au panneau d'interconnexion réseau. Son accès sera de préférence limité par une armoire fermée réservée aux responsables réseau.
- Réaliser toutes les opérations d'administration distante via des communications sécurisées (par exemple SSH, terminal serveur, etc.). L'objectif est de ne pas transmettre de paramètres d'authentification de compte d'administration en clair et sans protection.

TRAITEMENT DE L'INFORMATION

- Réserver l'installation et la gestion de l'infrastructure réseau à du personnel qualifié. Aucune connexion à l'infrastructure ne doit être possible sans l'intervention du personnel responsable (filtrage d'adresse Ethernet, désactivation des portes non-utilisées sur le commutateur, instauration de règles de filtrage firewall pour le trafic interne à l'organisation, etc.). En outre, tout ajout de systèmes de communication sans fil (Wi-Fi) devra être

associé à un chiffrement fort (WPA et non WEP) et les accès distants (VPN) seront soumis à un contrôle strict. Enfin, tout matériel de communication n'étant pas sous le contrôle total du gestionnaire sera proscrit (par exemple un modem sur les stations de travail).

- Réserver l'administration système à du personnel qualifié, appointé par l'organisation.
- Enregistrer toute tentative d'accès infructueux à des documents ou au système d'information (log).
- Analyser à intervalles réguliers les enregistrements des fichiers de logs. Cette analyse sera réalisée par du personnel compétent. En outre, il est indispensable que chaque système informatique synchronise son horloge avec une horloge de référence.

MESSAGERIE ELECTRONIQUE ET ACCES INTERNET/INTRANET/EXTRANET

- Soumettre tout mail (entrant et sortant) et tout document téléchargé à partir d'une source non fiable (Internet par exemple) à une détection des virus et code malicieux. Un outil de protection doit donc être présent sur chaque poste de travail. En outre, une centralisation de la gestion de ces outils doit impérativement être réalisée par les responsables informatiques et la mise à jour du logiciel doit être impérativement réalisée plusieurs fois par jour.
- Réaliser les échanges de courriers électroniques concernant des informations et documents à caractère sensible au moyen d'outils permettant le chiffrement des messages suivant un système à clé publique/clé privée. Tout échange de ce type devra en outre être associé à une signature électronique. L'administration des certificats se réalisera d'une manière centralisée par les gestionnaires informatiques.
- Vérifier lors de la mise en place d'un Intranet/Extranet qu'aucune porte dérobée n'a été ouverte. Avant toute mise en place d'un extranet, une ingénierie des communications réseau doit être réalisée afin de restreindre l'accès aux ressources exclusivement internes à l'organisation à des partenaires disposant des droits d'accès suffisants. De plus, un système d'audit doit être mis en place.
- Mettre en place un firewall. Cette mise en place se fera suivant le principe de la fermeture globale de toutes les entrées, suivie de l'ouverture des services requis.
- Traiter avec précaution tout courrier électronique non sollicité. L'administration informatique devra mettre en œuvre des outils (filtre anti-spam) au niveau du serveur de courrier afin de minimiser au maximum ce type de sollicitations.
- Tout document reçu depuis une source non identifiée doit être considéré comme suspect et immédiatement supprimé. La Direction Informatique doit en être informée.
- Vérifier les adresses de destination lors de l'envoi ou du suivi d'un courrier électronique.
- Mettre en place des systèmes évitant l'envoi de courriers électroniques de grande taille. Ces messages pourraient en effet bloquer toute autre transmission. C'est l'administration informatique qui est chargée de cette tâche (par exemple via une règle sur le serveur de courrier).
- Mettre en œuvre des outils d'analyse réseau afin d'identifier tout trafic ou comportement anormal. C'est l'administration informatique qui est chargée de cette tâche.

>>> A PROPOS DE L'AUTEUR

Patrice Kahn, ingénieur ISEP (1981), est gérant et fondateur de la société KSdF-Conseil. Il est consultant spécialisé dans la mise en œuvre des normes aéronautiques, ferroviaires, automobile, nucléaire, médical (DO 178B / DO178 C, DO 278, CEI 61508, EN 5012x, ISO 26262, CEI 60 880, CEI 62137, CEI 62304, ...).

Fort de plus de 30 ans d'expérience dans le domaine de la Sûreté de Fonctionnement des systèmes programmés, Patrice Kahn est Professeur Associé à l'ISTIA d'Angers. A l'Institut de Maîtrise des Risques (IMdR), il est animateur du GTR « Démarche et méthodes de Sûreté de Fonctionnement des logiciels ». Il est également membre du Bureau du Comité de programme des congrès LambdaMu 15, 16, 17 et 18.

Il a signé pour la revue « les Techniques de l'Ingénieur » un article sur la normalisation en matière de Sûreté de Fonctionnement des logiciels et il est co-auteur du livre « Anticipation, innovation, perception : des défis pour la maîtrise des risques à l'horizon 2020 ».

Cloud Computing et données personnelles : un risque à traiter impérativement

Par Bruno Rasle
Responsable du développement ISEP Formation Continue

Du fait des atouts annoncés (flexibilité accrue, réduction drastique des investissements, possibilité de se consacrer à ses métiers), ignorer le phénomène Cloud Computing et sa porte d'entrée qu'est le SaaS (Software-as-a-Service, distribution du logiciel comme un service via Internet) est devenu impossible pour une DSI. Mais des précautions essentielles doivent être prises dans le cadre d'un tel projet, notamment pour protéger les données à caractère personnel et se conformer à la loi Informatique et Libertés.

>>> L'INFONUAGIQUE

Le Cloud Computing est une nouvelle façon de consommer de l'informatique. Pour caractériser le phénomène, on distingue trois types de Cloud (privé, public, hybride), trois niveaux de service (SaaS – pour Software as a Service, IaaS – pour Infrastructure as a Service et PaaS – pour Plateform as a Service) et plusieurs singularités spécifiques (grande souplesse, accès via Internet, tarification à l'usage, mutualisation des ressources, etc.). La majorité des acteurs sont en train de basculer sur ce modèle et un grand nombre de nouveaux projets consacre d'ores et déjà « l'informatique dans le nuage ».

>>> LE CLOUD COMPUTING OBLIGE A REVISITER DES QUESTIONS DE FOND

Quelle que soit la façon de considérer le phénomène, de nouvelles problématiques voient le jour, comme la maîtrise des cycles de vie d'une instance, l'impact de la qualité du code sur le niveau de facturation, les règles de gouvernance ou la logique de tarification.

D'autres questions doivent être revisitées comme la souveraineté, la sécurité, la confidentialité, la traçabilité, la réversibilité des contrats et la conformité aux lois concernant la protection des données personnelles.

Sur ce dernier point, la CNIL (Commission Nationale Informatique et des Libertés) a mené une enquête avant de publier ses recommandations[1]. Son homologue britannique a fait de même, avec une approche très similaire[2].

La Commission commence par lister les principaux risques qui doivent être pris en compte : la perte de gouvernance sur le traitement, la dépendance technologique vis-à-vis du fournisseur de Cloud Computing, c'est-à-dire l'impossibilité de changer de solution (pour un autre fournisseur ou une solution interne) sans perte de données ; une faille dans l'isolation des données, c'est-à-dire le risque que les données hébergées sur un système virtualisé soient modifiées ou rendues accessibles à des tiers non autorisés, suite à une défaillance du prestataire ou à une mauvaise gestion du rôle d'hyperviseur ; les réquisitions judiciaires, notamment par des autorités étrangères, une faille dans la chaîne de sous-traitance, dans le cas où le prestataire a lui-même fait appel à des tiers pour fournir le service ; une destruction ineffective des données ou des durées de conservation trop longues ; un problème de gestion des droits d'accès par les personnes causé par une insuffisance de moyens fournis par le prestataire, l'indisponibilité du service du prestataire, ce qui comprend l'indisponibilité du service en lui-même mais aussi l'indisponibilité des moyens d'accès au service (notamment les problèmes réseaux) ; la fermeture du service du prestataire ou acquisition du prestataire par un tiers et la non-conformité réglementaire, notamment sur les transferts internationaux. Une liste plus complète de 35 risques fournie par l'ENISA[3] (European Network and Information Security Agency) peut aussi être utilisée.

[1] *http://www.cnil.fr/la-cnil/actualite/article/article/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services/*
[2] *http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/cloud_computing.aspx*
[3] *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing*

Sans surprise, la CNIL recommande de commencer par identifier et classifier les données et les traitements qui passeront dans le Cloud, de définir ses propres exigences en matière de sécurité, de conduire une analyse de risques (pour son entreprise mais aussi et surtout pour les personnes concernées) afin d'identifier les mesures essentielles à prendre, d'identifier le type de Cloud adéquat et de choisir en conséquence un prestataire présentant les garanties suffisantes.

>>> QUI EST RESPONSABLE DE QUOI ?

Cette question semble naïve, mais de sa réponse découle l'identité du responsable qui serait poursuivi, et éventuellement sanctionné, en cas de non-conformité. Au sens de la loi Informatique et Libertés, c'est sur le *Responsable de traitement* que pèse ce risque.

La logique veut que le Client soit systématiquement responsabilisé, la sous-traitance ne l'exonérant pas de ses obligations car en tant que donneur d'ordres, c'est lui qui décide de la finalité et qui fait appel à un prestataire. Toutefois, la CNIL constate que dans certains cas, les clients, bien que responsables du choix de leurs prestataires, ne peuvent pas réellement leur donner d'instructions et ne sont pas en mesure de contrôler l'effectivité des garanties de sécurité et de confidentialité. Cette absence de moyens de contrôle est due notamment à des offres standardisées, non modifiables par les clients, et à des contrats d'adhésion qui ne leur laissent aucune possibilité de négociation *(« Take it of leave it »)*.

Dans ces cas, une distribution des responsabilités peut être envisagée – le prestataire de Cloud pouvant se retrouver responsable (et donc sanctionnable) concernant la sécurisation des données personnelles traitées – mais la répartition des rôles et des responsabilités doit être très soigneusement formalisée dans le contrat qui lie les parties.

On rappellera qu'en effet, en vertu des pouvoirs qui lui sont conférés par la loi Informatique et Libertés, la CNIL peut contrôler (y compris sur site) et sanctionner tout responsable du traitement qui ne respecterait pas ses obligations. Par conséquent, si le client et le prestataire sont conjointement responsables du traitement, ils seront tous deux susceptibles d'être contrôlés et sanctionnés.

>>> LA QUESTION DES CERTIFICATIONS ET DES AUDITS

Il est indispensable qu'une entreprise française qui envisage de recourir à un service de Cloud Computing réalise une analyse de risques et soit très rigoureuse dans le choix de son prestataire. Il est recommandé de retenir un prestataire qui montre des signes tangibles de son sérieux, comme par exemple une certification ISO 27011 ou ISAE 3402 (qui a pris le relais de SAS 70 – *Statement on Auditing Standards n°70*). Mais certification ne veut pas dire conformité et ne remplace pas le besoin d'audit.

Dans ses « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud Computing », la CNIL propose une rédaction contractuelle : *« Le Client se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect par le Prestataire de ses obligations au titre du Contrat, notamment par le biais d'un audit. Le Prestataire s'engage à répondre aux demandes d'audit du Client et effectuées par le Client lui-même ou par un tiers de confiance qu'il aura sélectionné, reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du Prestataire, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit au Client. Les audits doivent permettre une analyse du respect du présent Contrat et de la loi Informatique et Libertés, notamment : par la vérification de l'ensemble des mesures de sécurité mises en œuvre par le Prestataire, par la vérification des journaux de localisation des Données, de copie et de suppression des Données, par l'analyse des mesures mises en place pour supprimer les Données, pour prévenir toutes transmissions illégales de Données à des juridictions non adéquates ou pour empêcher le transfert de Données vers un pays non autorisé par le Client. L'audit doit enfin pouvoir permettre de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié. »*

>>> DES AUJOURD'HUI INTEGRER LA NOTIFICATION DES VIOLATIONS

De même, la CNIL recommande de formaliser l'existence d'un système de remontée des plaintes et des incidents de sécurité : *« Le Prestataire s'engage à communiquer au Client la survenance de toute faille de sécurité ayant des conséquences directes ou indirectes sur le Traitement, ainsi que toute plainte qui lui serait adressée par tout individu concerné par le Traitement réalisé au titre du Contrat. Cette communication devra être effectuée dans les plus brefs délais et au maximum quarante-huit heures après la découverte de la faille de sécurité ou suivant réception d'une plainte. »*

Cette précaution s'explique aussi par l'intérêt qu'il y a à anticiper sur la promulgation du nouveau cadre légal européen : en janvier 2012 la Commission européenne a publié un projet de Règlement[1] qui – d'ici trois à cinq ans – viendrait remplacer la loi Informatique et Libertés.

[1] *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

Or ce projet obligera les responsables de traitement à informer l'Autorité de contrôle (la CNIL pour la France) et même chaque personne concernée d'une violation de ses données personnelles lorsque cette violation est susceptible de porter atteinte à sa vie privée.

De même, des précautions doivent être prises concernant la durée de conservation « *Le Prestataire s'engage à ne pas conserver les Données au-delà de la durée de conservation fixée par le Client au regard des finalités pour lesquelles elles ont été collectées, et en tout état de cause à ne pas les conserver après la fin du Contrat.* » et il faut prévoir un mécanisme efficient qui permette au client de s'assurer que les données ont bel et bien été purgées et ne risquent pas de réapparaitre dans le futur.

>>> OU SONT NOS DONNEES ET QUI Y A ACCES ?

On rappellera que, de par la loi Informatique et Libertés, les transferts de données personnelles hors Union Européenne sont par principe interdits, sauf exceptions prévues par le texte et sauf autorisations obtenues préalablement auprès de la CNIL. Cette règle, conçue à l'époque où la localisation des données était simple à établir, est mise à mal avec le concept de Cloud public dans lequel les informations sont dupliquées et déplacées dans de nombreux data centers répartis sur toute la planète.

Par conséquent, les organismes qui souhaitent migrer vers cette technologie doivent soigneusement sécuriser juridiquement ces transferts, de concert avec leur prestataire. La CNIL exige notamment des indications claires et exhaustives des pays hébergeant les serveurs du prestataire : « *Le Prestataire informe le Client que les Données seront hébergées dans des serveurs localisés dans les pays suivants : [fournir une liste exhaustive des pays hébergeant les serveurs du prestataire]. En cas de modification des pays destinataires par le Prestataire, ce dernier devra en informer préalablement le Client sans délai et obtenir son consentement écrit. Le cas échéant, le Prestataire devra fournir au Client une liste des pays destinataires mise à jour.* »

Il faut également prévoir les dispositifs nationaux qui permettent à certains gouvernements d'accéder aux données hébergés – comme le *Patriot Act* en cas de nécessité pour la sécurité nationale. En juin 2011 la communauté avait été émue par la réponse d'un grand acteur américain du Cloud Computing qui, en réponse à une question qui lui était posée lors d'une conférence, avait indiqué que son entreprise se verrait obligée de répondre à ce type de demande, même si les données visées étaient hébergées en Europe.

Enfin il est indispensable de mettre en place des procédures très strictes qui permettent de maîtriser et de tracer les accès des administrateurs techniques employés par les sous-traitants pour pouvoir répondre à la question « *Qui a accès à nos données ?* ».

>>> LA NEGOCIATION DU CONTRAT

On voit donc que les projets Cloud Computing demandent une grande vigilance concernant l'expression des besoins, la contractualisation la recette et les audits éventuels.

Le contrat devra fixer clairement les rôles et responsabilités de chacun, la sous-traitance en cascade – très fréquente dans le Cloud Computing – devra être sérieusement encadrée, la sécurisation et la confidentialité des données demandera une attention toute particulière.

D'autres sujets doivent être étudiés, comme la réversibilité/transférabilité (vers un autre Cloud Service Provider), la propriété intellectuelle, l'assurance de l'effectivité de la purge des données à l'issue du contrat, etc. Il faut également s'assurer que le prestataire ne pourra pas utiliser les données confiées à d'autres fins, par exemple publicitaires.

>>> LA COMMISSION EUROPEENNE VEUT AVANCER SUR LE SUJET

Le 27 septembre 2012 la Commission européenne a dévoilé sa stratégie numérique dans un document intitulé « *Nouvelles mesures pour stimuler la productivité des entreprises et des administrations de l'UE grâce à l'informatique en nuage*[1] ». Elle y annonce notamment vouloir rapidement définir les normes techniques nécessaires à l'interopérabilité, la portabilité des données et la réversibilité pour les utilisateurs du Cloud, soutenir les systèmes de certification à l'échelle de l'Union européenne pour les fournisseurs de services Cloud fiables, mettre en œuvre un modèle type de conditions contractuelles « *sûres et équitables* ». La Commission européenne s'est fixé pour objectif de créer 2,5 millions d'emplois liés au Cloud Computing et de stimuler le PIB de 160 milliards d'euros d'ici 2020. L'institution indique que les avantages du Cloud proviennent de ses économies d'échelle, précise que 80% des entreprises qui l'adoptent font 10 à 20% d'économies et qu'une large adoption de cette technologie dans tous les secteurs de l'économie pourrait entraîner des gains de productivité importants.

[1] *http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/1025&format=PDF&aged=0&language=FR&guiLanguage=en*

Cloud Computing et données personnelles : un risque à traiter impérativement

>>> A PROPOS DE L'AUTEUR

Bruno Rasle a participé à la création de la première entité française dédiée à l'optimisation des réseaux et à la gestion des performances en environnement IP et s'est consacré ensuite à la protection des données stratégiques. Auteur du livre « Halte au Spam », il a été membre du groupe de contact anti-spam mis en place par la DDM (Direction du Développement des Médias, services du Premier ministre). Bruno Rasle est Délégué Général de l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel) et intervient dans le cadre du Mastère Spécialisé « Management et Protection des Données à caractère personnel » de l'ISEP (Institut Supérieur d'Électronique de Paris).

Vers un modèle d'intelligence de crise : Les outils d'aide à la préparation de l'imprévu

par Diane Rajaona
Titulaire du Mastère Spécialisé en Intelligence des Risques et des Opportunités par l'Intelligence Économique de l'ISEP - Consultante en gestion des risques - ARSéO

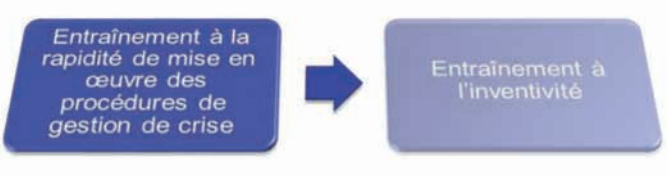
Aujourd'hui, l'enjeu des entreprises est de piloter leur activité vers une logique de performance globale et durable intégrant tous les autres indicateurs de coût, de qualité, de délai et… de risques. Au départ, la gestion de risques est intra-muros et concerne l'activité de l'entreprise en termes d'organisation, de processus, de ressources et de produits/services. Très rapidement, cette gestion de risques englobe aussi des facteurs « environnementaux » au sens large (risque concurrentiel, risque technologique, risque sociétal, risque réglementaire, etc.). L'intelligence des risques permet ainsi de développer une approche anticipative et préventive des risques de façon globale et intégrée.

>>> INTRODUCTION

Virus H1N1, suicides sur le lieu de travail repris dans les médias, fermetures surprise de grands sites industriels, rappels de produits défectueux, pollutions majeures, explosion sur le site AZF en 2001, attentats du 11 septembre 2001, nuage volcanique islandais qui a traversé le ciel européen en avril 2010, inondations dans le Var en juin 2010, tornade à New York en septembre 2010, accident nucléaire de Fukushima suite au séisme du 11 mars 2011 de magnitude 9 qui a déclenché un tsunami, explosion de la bulle de la dette européenne en août 2011. Les origines de toute crise apparaissent variées, difficilement prévisibles et pourtant fréquentes à l'échelle nationale, européenne voire planétaire.

Selon un article paru dans Les Échos[1], ces crises sont de type non conventionnel ou « hors cadre » et se caractérisent par des « discontinuités brutales ». Leur ampleur se trouve renforcée par un effet de propagation instantané en raison des sociétés modernes qui *sont faites d'ensembles interconnectés, interdépendants, favorisant les effets dominos ultrarapides*. A cela, il faut ajouter la dispersion géographique de la crise dans un contexte de globalisation.

Au regard de cette grande tendance, l'enjeu n'est plus de maîtriser la mise en œuvre des procédures de gestion de crise pour atténuer les impacts d'une situation de crise, sauvegarder les actifs (matériels, humains, financiers, informationnels…) ni de procéder au plus vite aux opérations de redémarrage des activités essentielles dans une optique de retour à une situation nominale. A présent, le véritable enjeu est de concevoir des outils d'aide à la préparation de l'imprévu permettant de s'entraîner à être inventifs ensemble pour penser autrement les scénarios de crise et mieux fréquenter l'inconnu.



>>> OBJECTIF

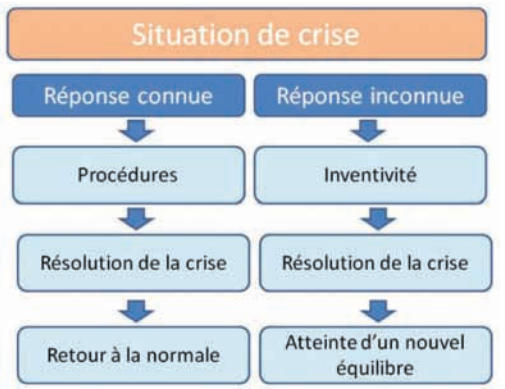
Concrètement, il s'agit de donner au décideur une boite à outils dédiée aux crises dites impensables afin de lui permettre :

- d'utiliser une méthode opérationnelle qui fait sortir des sentiers battus malgré une situation de stress peu propice à la créativité ;
- de cesser d'être surpris ;
- de ne pas se trouver dans une situation telle qu'il n'y ait plus rien à faire.

[1] *Les Échos du 4 novembre 2005 - Page 19, « Grippe aviaire : une crise de pilotage », Xavier Guilhou et Patrick Lagadec*

Vers un modèle d'intelligence de crise : Les outils d'aide à la préparation de l'imprévu

En parallèle, il s'agit aussi de compléter l'outillage existant fondé sur des procédures (ou réponses connues) au sein des entreprises pour pouvoir faire face aux crises conventionnelles qui risquent de se transformer soudainement en événement inconcevable par effet de mutation pour lequel la réponse est inconnue :



>>> DESCRIPTION DU MODELE D'INTELLIGENCE DE CRISE

Notre modèle d' « intelligence de crise » est né de l'application de l'intelligence inventive à la gestion de crise. Ce modèle est transverse aux phases amont et aval de la gestion de crise conformément au schéma suivant :

L'intelligence de crise a pour double objectif de :
- pérenniser la protection de l'entreprise à travers le concept d'« entreprise protégée »
- porter sur la gestion de crise un regard d'innovation.

Ces objectifs permettent de répondre aux enjeux suivants :
- Comment attaquer la situation de crise sous un angle approprié ?
- Comment formaliser la crise à résoudre ?
- Comment générer de nouvelles idées ?
- Comment valoriser les idées ?

En amont de la gestion de crise, il a été mis en place un outil d'autodiagnostic de 112 questions organisées autour de 12 mots clés de l'intelligence inventive :

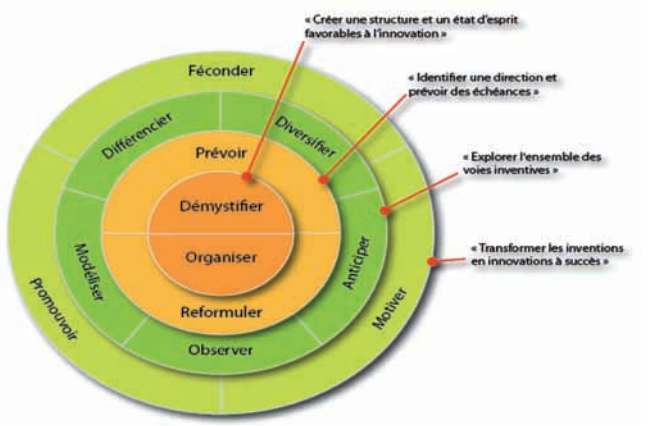


Schéma Bernard BESSON et Renaud UHL

L'objectif de cet outil d'autodiagnostic est d'aider les membres du dispositif de crise et les différents services à l'appui à imaginer différemment ce qui pourrait arriver à leur entreprise en matière de sinistre ou de crise. L'enjeu de pouvoir discerner des questions vitales et de penser à des crises insoupçonnées est primordial dans la mesure où la survie de l'entreprise est l'affaire de tout le personnel de l'entreprise.

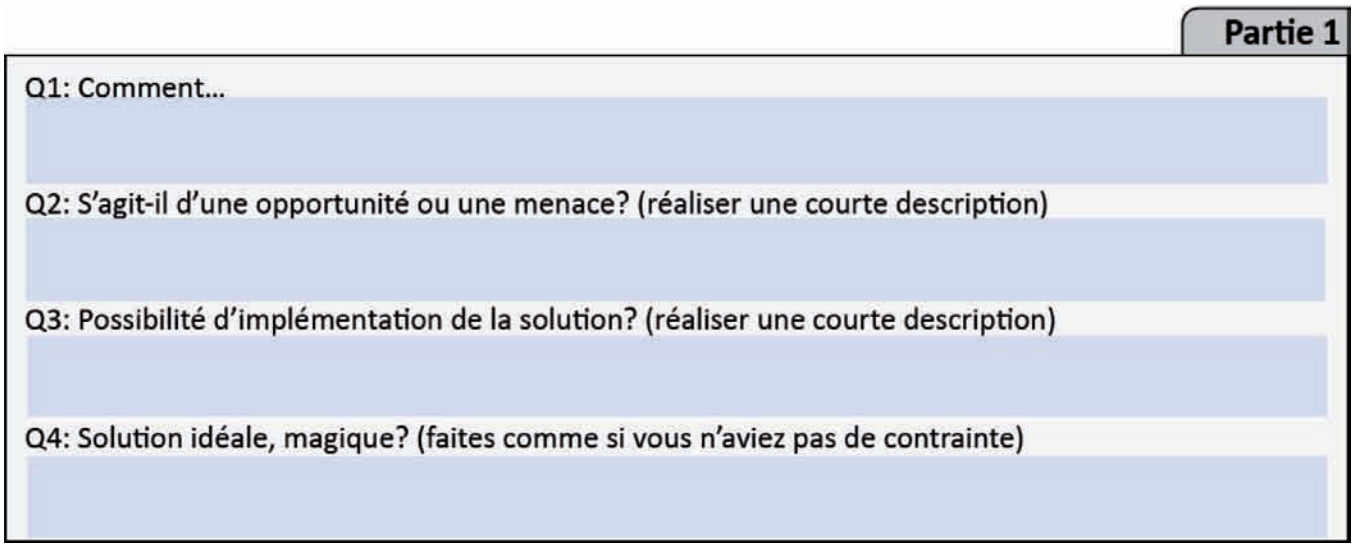
Concrètement, il s'agit :
- d'identifier les points bloquants à la démarche de gestion de crise de l'entreprise concernée à travers la réalisation d'un autodiagnostic ;
- de réfléchir en permanence sur la pertinence, la cohésion et les objectifs qui ont été assignés à l'intelligence de crise de l'entreprise ;
- de visualiser et de s'approprier des méthodes simples et efficaces ;
- de partager une vision consensuelle de la gestion de crise ;
- d'initier le dialogue à travers un langage partagé ;
- de définir un plan d'action en 12 étapes visant l'atteinte d'un niveau de maturité supérieur ;
- de piloter les crises hors cadre avec succès.

En aval de la gestion de crise a été mise en place une démarche de modélisation de la situation de crise :

Pour bien comprendre les tenants et aboutissants de cette démarche, un cas pratique a été développé. Nous allons considérer l'existence fictive d'une grande enseigne gérant plusieurs marques de vêtements au niveau national. Suite à un bogue sévère de son logiciel de paye, des retards de paiement de plusieurs mois affectent des employés qui constituent la catégorie la plus fragile financièrement. Pour tenter de résoudre cette crise technique qui pourrait se dégénérer en crise sociale sans précédent, l'enseigne va recourir au mode opératoire « Domino » qui se déroule comme suit :

PRENDRE UNE BONNE DIRECTION

La reformulation du problème permet de s'assurer qu'un état non souhaité est un problème en lui-même ou non. Un changement de perception du problème est alors amorcé pour identifier l'angle d'attaque le plus approprié. En vue de converger vers une nouvelle solution viable à partir d'un affinement itératif de la problématique à traiter, le recours au mode opératoire « Domino » est utile. Il s'agit d'un questionnaire divisé en trois parties dédiées à l'exploration de notre problématique initiale de façon interrogative. Le point de départ (Q1) de cette analyse consiste à formuler le problème initial de façon interrogative, puis à répondre à l'ensemble des questions de la partie 1 comme suit :



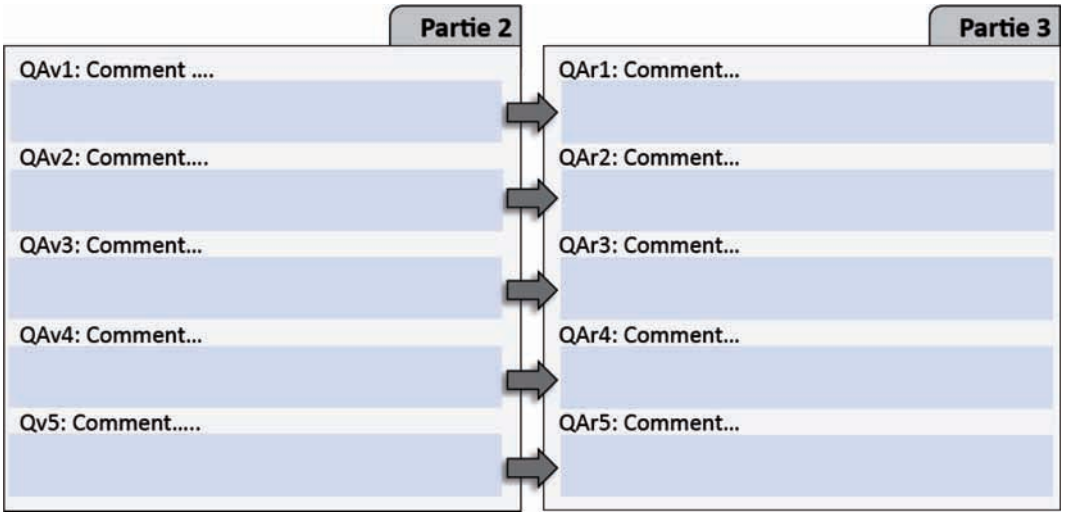
Mode opératoire Domino – Partie 1

Q1 : Comment faire pour que le retard de paiement ne soit pas préjudiciable ?
Q2 : Comment saisir une opportunité d'atténuement des impacts sociaux suite à la réalisation d'un risque de discontinuité du système d'information de paye construit et mis en service par l'enseigne au niveau national ?
Q3 : Comment s'assurer que les mesures techniques implémentées (procédure de bascule, construction d'un site de secours informatique, etc.) soient 100% opérantes en cas de sinistre survenu au dernier jalon du calendrier de paye (1er au 8 du mois M+1) qui est la période charnière de mise en paiement de tous les employés de l'enseigne ?
Q4 : Comment rendre le risque de discontinuité nul ?

Dans la partie 2, le « porteur du problème » est invité à reporter ou à reformuler, si nécessaire, en QAv1 sa question initiale en tenant compte des éléments nouveaux apportés par la partie 1. En QAv2 il imaginera ensuite, en le formulant de façon interrogative, le problème qu'il devra affronter une fois la problématique précédente (QAv1) traitée. Il procèdera de même en QAv3, QAv4 et QAv5.

Dans la partie 3, le « porteur du problème » est invité à s'interroger sur le bénéfice que génère la résolution du problème situé en face (Ex: QAv3 et QAr3). Il formulera ensuite ce bénéfice sous forme interrogative.

Autrement dit, QAv correspond à un problème à résoudre : comment le résoudre dans l'immédiat ? QAr correspond à un problème qui a déjà été résolu : quel est le bénéfice de cette résolution et/ou comment agir pour trouver une façon pérenne de ne plus le rencontrer ?



Mode opératoire Domino – Parties 2 et 3

QAv1 : Comment l'enseigne doit-elle neutraliser le risque de discontinuité de l'activité de paye ?	QAr1 : Comment l'enseigne peut-elle promouvoir son image en tant que modèle exemplaire de la distribution des vêtements ?
QAv2 : Comment l'enseigne doit-elle faire pour que le retard de paiement ne soit pas préjudiciable ?	QAr2 : Comment l'enseigne peut-elle atténuer les impacts financiers et sociaux ?
QAv3 : Comment l'enseigne peut-elle prendre en charge les difficultés de fin de mois des employés les plus sensibles en cas de non-paiement ?	QAr3 : Comment prendre en charge les factures mensuelles à régler (loyer, électricité-gaz, échéancier de crédit à la consommation, etc.) ?
QAv4 : Comment l'enseigne peut-elle améliorer le contexte socio-économique des employés les plus sensibles ?	QAr4 : Comment l'enseigne peut-elle accroître le bien-être social au sein des différentes marques gérées par elle ?
QAv5 : Comment l'enseigne peut-elle s'inscrire dans une logique de développement des ressources humaines sur le long terme ?	QAr5 : Comment l'enseigne peut-elle créer de la valeur ajoutée sur toute la chaîne des ressources humaines ?

A travers le mode opératoire Domino, le fait d'expliciter les problèmes sous forme de questions débutant par « Comment…» ou « Par quel » est une technique astucieuse qui permet de garder une ouverture d'esprit et ainsi d'inviter au dialogue. Autrement dit, il s'agit d'examiner en premier lieu les forces ou les bénéfices légitimes de la résolution d'une problématique afin d'éviter de répondre par le réflexe négatif à une nouveauté.

Après avoir renseigné le mode opératoire Domino, il est dorénavant possible de développer une meilleure compréhension du point précis où concentrer l'énergie des acteurs du dispositif de crise d'une organisation et éventuellement découvrir les questions qui peuvent être réellement au cœur de la crise.

FORMALISATION DU PROBLEME

La formalisation du problème se fait dans le cadre d'un champ d'exploration restreint en listant les objets liés au système socio-économique impacté par la situation de crise. Autrement dit, plus nous sommes contraints, plus nous devenons créatifs.

Ces objets sont des *ressources* liées à l'environnement immédiat du problème ou de la situation de crise. Ces ressources peuvent être matérielles (objets), humaines, financières, informationnelles et sont situées dans le système, l'espace et le temps. La condition du monde clos (ou de l'environnement immédiat) consiste à se servir des objets identifiés dans la phase d'analyse du problème puis à caractériser :

- les liaisons qu'ils ont entre eux,
- leur fonction (effet désirable),
- leur anti-fonction (effet non désirable) si existante,
- les attributs qui les définissent.

Une solution créative se traduit concrètement par un moyen qui permettrait de faire en sorte que l'effet négatif soit rendu indépendant du facteur d'aggravation, voire d'inverser le lien. A des fins de démonstration, nous allons nous concentrer uniquement sur l'objet « personnel » et observer des liens (contradictoires ou non) que ses attributs entretiennent avec le problème de « retard de paiement » (effet non désiré).

Le changement qualitatif nous invite à trouver un moyen qui permettrait de faire en sorte que l'effet du retard de paiement soit d'autant plus neutre que le nombre d'employés sensibles est élevé d'où le deuxième schéma suivant :

CREATION DE CONCEPTS INVENTIFS :

De façon générale, en s'inspirant de la méthode USIT (Unified Structured Inventive Thinking), il existe cinq méta-principes pour générer de nouvelles solutions en groupe de travail collectif :

Unification	Résolution du problème en utilisant un objet du monde clos et en lui donnant une nouvelle fonction ou une fonction complémentaire.
Multiplication	Résolution du problème en insérant dans le système actuel une copie légèrement modifiée d'un élément du monde clos. Pour identifier des critères pertinents de multiplication, il peut être intéressant de se servir de la méthode du changement qualitatif.
Division	Résolution d'un problème en divisant un objet existant du monde clos et en réorganisant ses parties.
Asymétrie	Résolution d'un problème en rompant l'homogénéité d'un objet.
Suppression	Résolution d'un problème en éliminant un objet ou un de ses composants.

Les 5 méta-principes

VALORISATION DES IDEES

A l'origine, les idées sont vulnérables. Cela dit, une fois que la liste des solutions ou options a été dressée, il faut identifier l'essentiel de ce que l'option a d'unique en posant systématiquement la question suivante : *Quelle(s) qualité(s) possède cette option qu'une autre ne possède pas ?* afin de préserver la nouveauté de l'option. Pour notre cas, les qualités seront surtout d'ordre organisationnel et humain car rappelons-le, notre système n'est pas technique, il est de nature socio-économique.

Par la suite, l'étape d'évaluation permet d'apprécier et de sélectionner les solutions les plus pertinentes produites sur la base de critères logiques (attractivité, faisabilité, coût, rapidité de mise en œuvre, etc.) au regard des objectifs fixés mais aussi au regard de la mise à l'épreuve par rapport à une situation de crise donnée.

>>> CONCLUSION

Le monde moderne semble favoriser les crises majeures et multipolaires. Ainsi, les sphères économiques, politiques, technologiques, environnementales, sociales connaissent simultanément de profondes mutations qui sont souvent issues de la conjonction de multiples, faits pourtant de faible ampleur. Il s'agit de crises inédites ou encore non conventionnelles qui s'inscrivent en dehors des modes opératoires des organisations et bouleversent leur cadre de référence. Pour cette raison, nous recommandons à tout dispositif de crise de réagir de façon rapide, simple et innovante face à une situation de crise majeure, quelles que soient ses origines de survenance.

En appliquant l'intelligence de crise aux quatre familles de risques (sécurité, sûreté, environnement et management), on vise à atteindre une résilience globale de l'entreprise.

>>> A PROPOS DE L'AUTEUR

Après avoir mené de nombreuses missions dans les domaines de la veille stratégique, la sécurité, la gestion des risques, de crise et de continuité d'activité, **Diane Rajaona** a préparé le Mastère Spécialisé *Intelligence des Risques et des Opportunités par l'Intelligence Économique* dispensé par l'ISEP en 2010 pour pouvoir répondre à l'enjeu principal des sociétés modernes.

Responsabilité sociétale des entreprises et cartographie des risques

par Séverine Cartot
Titulaire du Mastère Spécialisé en Intelligence des Risques et des Opportunités par l'Intelligence Économique de l'ISEP
Solsequia Finance

La Responsabilité Sociétale des Entreprises prend plus d'importance avec la publication du décret du 24 avril 2012 relatif aux obligations de transparence des entreprises en matière sociale et environnementale de l'article 225-102 du code de commerce : l'information est-elle abordée par les entreprises comme un exercice de communication ou comme une démarche stratégique de gestion des risques globale ?

>>> LES ORIGINES DE LA RESPONSABILITE SOCIETALE DES ENTREPRISES

Depuis les années 60, l'économie mondiale est entrée dans une phase d'accélération de la production, facilitée par le développement de la société de consommation et la croissance démographique mondiale. Il en résulte : consommation des ressources, accélération des inégalités mondiales entre le nord et le sud, apparition de nouveaux risques sanitaires (grippe aviaire, vache folle, cancers), réchauffement climatique (tempête, sécheresse, ouragan), accidents industriels d'envergure mondiale. La nature des risques a donc évolué.

Aussi, quelques visionnaires ont-ils, à la fin des années 80, fait émerger le concept de développement durable. Conscients des conséquences néfastes potentielles au niveau environnemental et social et des enjeux générés par l'accélération de la production des richesses au détriment des ressources planétaires, ces derniers ont défini ce concept qui repose sur le principe de répondre aux besoins du présent, sans compromettre les capacités des générations futures.

Autrement dit, que pouvons-nous faire pour laisser à nos enfants une planète aussi propre que celle que nous avons trouvé ?

Le sommet de la Terre à Rio de Janeiro en 1992 a marqué l'avènement de la naissance de ce concept. Celui-ci repose sur un modèle de développement qui intègre à la fois des aspects écologiques, économiques et sociaux :

- L'intégration des contraintes écologiques dans un modèle économique à long terme est à l'origine d'un modèle viable ;
- L'intégration d'un modèle économique créateur de richesse et source de développement dans une société génère un environnement équitable ;
- L'intégration de facteurs écologiques au sein d'un groupe d'individus régi par des relations sociales et solidaires est qualifiée d'environnement vivable.

Le défi consiste à lier ces trois axes dans un modèle de développement à long terme, par opposition à une société de consommation où l'éphémère est omniprésent : cet équilibre est appelé **développement durable**.

En 2012, vingt ans après le Sommet de la Terre, le concept s'est vulgarisé et nous entoure au quotidien, au même titre que le phénomène de consommation. Grâce à la multiplication des normes et conventions, la soft law relative au développement durable s'est développée mais elle reste incitative. Cet aspect est en cohérence avec la politique de responsabilité du développement durable. La prise en compte de ces enjeux par les entreprises est dénommée **Responsabilité Sociétale des Entreprises** (RSE).

>>> LA RESPONSABILITE SOCIETALE DES ENTREPRISES COMME CARTOGRAPHIE DES RISQUES EXTRA-FINANCIER DE L'ENTREPRISE

Que ce soit le reflet d'une démarche légale ou volontaire, la plupart des grandes entreprises communiquent aujourd'hui de plus en plus sur ce thème. Certaines PME en font même une valeur ajoutée par rapport à leurs concurrents. A l'origine, le concept du développement durable est né en réponse à une prise de conscience des risques inhérents à chacun des trois axes économie, écologie, société. On peut se demander si ces risques sont aujourd'hui réellement pris

en compte, ou s'il s'agit d'un exercice de communication d'entreprises soucieuses de leur image. Que veut dire prendre en compte la RSE pour une entreprise ? Comment l'appréhender ? Comme un exercice de communication et un passage obligé pour répondre à des obligations légales de communication d'informations ? Comme un département support complémentaire dans l'organisation d'une entreprise structurée en silo ? Ou encore, comme un outil de maîtrise globale des risques, intégré à la stratégie globale de l'entreprise ?

C'est selon cette dernière approche que j'aborderai la RSE. En effet, la législation donne une place non négligeable à la gestion des risques au sein de la gouvernance d'une entreprise : l'article L 225-100 du code du commerce fait obligation au conseil d'administration de rendre compte des risques dans son rapport de gestion qui doit notamment comporter une description des principaux risques et incertitudes auxquels la société et les sociétés qu'elle contrôle sont confrontées. La gestion des risques est donc un sujet à part entière : ce dispositif repose sur l'identification des risques, leur analyse, puis leur traitement. Il suppose un processus de pilotage en continu afin d'assurer son amélioration

La RSE, quant à elle, met l'accent sur la maîtrise de risques non financiers. Aussi, devant l'importance croissante de la cartographie des risques, la RSE apparait comme une démarche stratégique de prévention des risques et donc de performance.

La RSE est une démarche globale qui implique la prise en compte des facteurs environnementaux, sociaux et financiers dans les actions de l'entreprise. Elle repose sur une vision à moyen, long terme et induit une autre façon de compter : quels sont les coûts indirects d'une action sur l'environnement, les ressources de l'entreprise, la société ? Elle prend également en compte les risques extra-financiers (comme l'image, la réputation), humains ou juridiques, ou les savoir-faire. L'ensemble de ces éléments, constitutifs du capital immatériel de l'entreprise, ont également une incidence sur les performances financières de l'entreprise. Elle permet donc de concilier croissance et équilibre, respect de l'environnement, développement et innovation, valorisation des ressources, concurrence et performance.

>>> LA COMMUNICATION DES ENTREPRISES SUR LA RSE

Les rapports annuels des entreprises cotées sont une source importante d'information pour apprécier l'approche RSE des entreprises et le positionnement de ce thème, même si l'information reste une matière fragile, sensible et modelable.

La démarche reflétée à travers les publications des entreprises est-elle cohérente avec la démarche globale du développement durable ? Pour chacun des trois piliers, la prise en compte des différents risques, leur mise en exergue, et les réponses apportées sont-elles présentes d'une part, traduisent-t-elles une réalité d'autre part ?

Quelques exemples permettent de montrer la diversité de la réalité de la prise en compte de la RSE par les entreprises.

On peut citer, sur le plan environnemental, l'entreprise LU, qui a mis en place la Charte LU'Harmony. Issu d'un ingrédient millénaire, le blé, LU a mis en place une démarche innovante qui concilie partenariat avec des fournisseurs, une culture de qualité, la traçabilité et respect de l'environnement : le blé est cultivé à proximité des sites de production selon des pratiques exigeantes pour une production de qualité. Deux à trois pour cent de la surface est consacrée à une bordure fleurie afin de permettre aux abeilles et papillons de se nourrir du pollen dont ils ont besoin. Enfin, la traçabilité est assurée à toutes les étapes du processus de production.

A l'inverse, le groupe de chimie Rhodia, poursuivi par un lourd passé de pollueur, fait part d'objectifs ambitieux de réduction de gaz à effet de serre alors que certains sites de production sont référencés comme pollués. Ces objectifs importants traduisent certes la volonté de progrès du groupe mais aussi l'ampleur de la problématique de la pollution dans cette industrie.

L'industrie pétrolière n'est pas en reste avec des accidents de marée noire ou défaut de maintenance de plateforme à l'origine de catastrophes lourdes de conséquences environnementales et financières.

Au niveau social, l'entreprise Leroy Merlin, lauréate en 2011 pour la septième année consécutive selon le palmarès « Greatplacetowork », a fait de ce risque un atout compétitif et affiche sa culture basée sur le partage, l'autonomie et le collectif. Les dépenses de formation représentent près de 7% de la masse salariale contre une moyenne de 1% pour les entreprises françaises.

Au chapitre des délocalisations et restructuration, l'exemple de Nike a fait également fait couler beaucoup d'encre en 2003 : la multinationale a alors présenté la liste de la localisation de ses ateliers de production dans le monde. Parmi les 700 usines, à cette date, 124 se trouvaient en Chine, 74 en Thaïlande, 34 au Vietnam. Un audit diligenté par Nike révéla des cas de harcèlement physique ou verbal, de travail des enfants, ainsi que des conditions de travail parfois très difficiles. Depuis, l'entreprise se positionne sur le développement durable par la conception d'une chaussure mêlant matériaux recyclés et éco-matériaux.

La BNP, qui avait obtenu le label de la diversité attribué par l'AFNOR en 2009 pour trois ans, a quant à elle été condamnée en 2010 pour discrimination envers l'une de ses ex-salariées en raison de son sexe, de sa grossesse et de sa situation de famille. La banque avait en effet signé un accord sur l'égalité professionnelle entre les femmes et les hommes destiné notamment à *respecter le principe fondamental d'égalité de traitement notamment en termes de rémunération*[1].

En matière de lutte contre la corruption, le guide de conformité de Siemens constitue un exemple. En effet, suite à des mises en cause, le groupe s'est engagé dans une véritable politique anti-corruption qui se traduit par des contrôles de conformité internes clairement définis.

Le concept du développement durable a donc pris une large ampleur et fait désormais partie de notre quotidien de consommateurs ainsi que celui des entreprises dans une mesure plus ou moins importante ; alors que certaines en ont fait la base de leur stratégie, d'autres s'efforcent d'y adhérer.

>>> EVOLUTION ET MARGE DE PROGRES DE LA RSE

A travers l'étude des trois piliers, force est de constater que l'appréhension des risques est très variable, et parfois contradictoire, avec les actions réelles des entreprises. Le premier biais est constitué par l'information elle-même : parfois surabondante via la publicité ou le marketing, le consommateur est souvent noyé dans des terminologies impropres, et déclinées bien plus souvent que de raison. Le rôle des ONG, de l'État, est alors primordial pour lutter contre ces abus. Dans un second temps, la collecte de l'information s'avère être un exercice complexe dans des organisations où la réalisation d'objectifs va tendre vers le but premier de l'entreprise, la réalisation du profit. Enfin, l'analyse de ces informations est complexifiée par l'absence de référentiel, leur caractère souvent immatériel, leur mesurabilité et vérifiabilité effectives. Les agences de notation extra-financières sont donc un gage important de la fiabilité des informations, et du positionnement sectoriel des acteurs, ainsi qu'un vecteur d'influence : le pouvoir de sanction vis-à-vis des entreprises engagées dans une démarche RSE et incluses dans les indices de notation extra-financiers n'est pas neutre car elle peut engendrer une sortie de cote.

L'analyse des publications RSE permet d'apprécier dans quelle mesure les entreprises appréhendent les risques et mettent en place une démarche de développement durable. Les exemples positifs existent, mais les contre-exemples sont nombreux dans chacun des domaines et les lacunes flagrantes, dans un contexte économique qui valorise les performances à court terme. La faiblesse de l'investissement ISR (Investissement Socialement Responsable) et le manque de soutien des banques ne favorisent pas les démarches RSE des entreprises. Ces dernières, parfois peu cohérentes, mettent en avant les innovations technologiques au détriment du dialogue avec les parties prenantes : leur politique anti-corruption, alors qu'elles sont prises en faute par rapport à l'égalité homme-femme, ou pire, sont parallèlement condamnées en justice pour corruption. D'autres se targuent de développer des filières de distribution Bio au détriment d'un bilan carbone peu flatteur, à l'encontre du principe de proximité. Enfin, les grands pollueurs s'enrichissent également grâce au marché de la dépollution… Performante dans un domaine, l'intégrité de la démarche est complexe à mettre en œuvre dans sa globalité pour une même entreprise. De plus, ces entreprises, qui s'exposent par leur communication, sont vite prises en défaut par la presse ou les ONG.

Le développement durable se veut avant tout être une démarche progressive, et chaque entreprise, en fonction de son tropisme initial, de son métier, de sa stratégie, fera valoir ses avancées technologiques, ses performances sociales ou la qualité de sa gouvernance, alors qu'elle est relativement peu avancée sur les autres aspects. La difficulté réside en l'appréhension de la démarche, dans une même mesure pour chacun des trois axes. La maturité de la démarche s'apprécie donc sous l'angle d'un équilibre global : le commerce équitable, lui, néglige les aspects économiques, d'autres minimisent les aspects sociaux, et les syndicats ont du mal à se positionner face à la RSE. Rares sont les entreprises qui, à l'instar de Nature et Découverte «entreprise du commerce de demain », ont fondé intégralement leur stratégie sur le développement durable. Distributeur de produits « soucieux de la naturalité », promouvant l'éthique et la citoyenneté dans une entreprise de la connaissance, le cœur de métier est décliné globalement sur un modèle de développement durable.

L'absence de sanctions des entreprises vis-à-vis des performances RSE est un frein considérable. En effet, les avancées en la matière résultent de mises en cause et conséquences financières lourdes suite à des scandales de corruption ou d'images susceptibles d'influencer directement les consommateurs, de dégrader la cote financière et extra-financière des entreprises en bourse, donc de diminuer la rentabilité des entreprises.

Cependant la démarche RSE semble être de plus en plus prise en compte et, au même titre qu'elle apparait dans le

Top Ten des risques les plus cités par les entreprises, le 7ème bilan des assemblées générales établi par l'agence de notation extra-financière Capitalcom montre que les préoccupations sociétales deviennent une véritable réalité pour le management dans un contexte de crise économique : « la moitié des grandes entreprises ont présenté leur politique de responsabilité sociale comme une composante majeure de la croissance » Ainsi, la RSE est un sujet de plus en plus abordé par les dirigeants qui les associent aux présentations stratégiques lors des assemblées générales. Le capital humain est lui présenté comme un relais de croissance et non plus comme un coût.

La gestion des risques et leur prévention, quant à elles, suscitent de plus en plus de questions de la part des actionnaires. Rares sont les entreprises qui présentent une cartographie de leurs risques et qui expliquent les procédures d'anticipation et de gestion prévisionnelle des risques. Michelin, Air Liquide ou Accor font figure de pionniers en la matière.

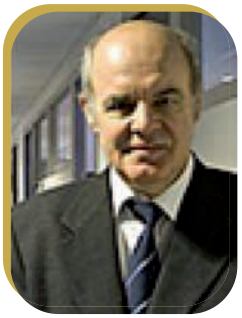
Cependant cette tendance pourrait être amenée à s'inverser dans les années à venir : en effet, le 25 octobre 2011 la Commission Européenne a communiqué sa nouvelle stratégie pour la RSE pour la période 2011-2014. Celle-ci est présentée comme un outil de performance, un avantage concurrentiel et une solution à la crise. La Commission Européenne envisage ainsi une harmonisation des politiques RSE des états membres, qui deviendrait alors un outil de régulation économique. La RSE ne serait plus du seul ressort des entreprises mais aussi des États.

>>> A PROPOS DE L'AUTEUR

Séverine Cartot est fondatrice et associée de Solsequia Finance. Elle est expert-comptable et commissaire aux comptes, diplômée ès sciences-économiques de l'Université Panthéon Sorbonne.

Après treize ans d'expérience en cabinet d'audit et expertise-comptable, elle a préparé le Mastère Spécialisé en Intelligence des Risques et des Opportunités par l'Intelligence Économique de l'ISEP. Au cœur du traitement de l'information financière de par son métier, pour la produire ou la contrôler, l'information financière apparait comme une matière première riche à analyser et maîtriser pour réduire l'incertitude liée au risque auquel les entreprises sont exposées. Savoir la transmettre apparait donc comme la première qualité de l'expert-comptable.

Depuis, elle a créé son propre cabinet Solsequia Finance, où qualité et communication vont de pair !



Cyber escarmouches ou état de cyberguerre, un risque majeur

par Gérard Peliks
Président de l'atelier sécurité de Forum ATENA
Intervenant dans des Mastères spécialisés de l'ISEP

L'information, les systèmes d'information, les réseaux connaissent aujourd'hui des attaques répétées, de plus en plus violentes, exécutées par des vecteurs très sophistiqués. Ces attaques n'ont pas pour but la recherche d'un gain pécuniaire mais plutôt tentent de dérober des informations sensibles ou de compromettre les infrastructures vitales des pays ciblés. On ne parle pas alors de cybercriminalité, ce sont les pays et leurs citoyens, les entreprises et leurs employés qui sont visés. Mais peut-on pour autant qualifier cet état de « cyberguerre » ? La guerre dans le cyber espace aura-t-elle lieu ?

Plus un pays est avancé dans l'utilisation des technologies du numérique, plus il est fragilisé, car le combat, au moins aujourd'hui, est un combat asymétrique où le faible peut faire d'autant plus de dégâts chez son adversaire qu'il est fort. A ce risque s'ajoute bien sûr la possibilité pour le fort de répliquer par des représailles qui sortent du domaine de la guerre virtuelle.

2012 est l'année de tous les dangers. Tout s'accélère côté attaques menées par des maliciels très sophistiqués, mais revenons d'abord quelques années en arrière.

2007, l'Estonie, un des pays les plus avancés en Europe dans l'utilisation des technologies du numérique par sa population, a été la cible d'attaques simultanées en dénis de services distribués (DDOS), provenant de plusieurs dizaines de pays, et qui ont abouti à l'isolement de cet état et à l'impossibilité pour les Estoniens d'accéder à leurs administrations, à leurs services bancaires, aux services de télécommunication et aux numéros d'urgence. Que s'était-il passé ?

On a pu constater que ces attaques avaient été déclenchées suite au déplacement, à Tallinn, d'une statue érigée à la mémoire du soldat soviétique lors de la deuxième guerre mondiale. Cette action déplut fortement à la communauté russophone d'Estonie. Des sollicitations multiples vers les serveurs Web estoniens affluèrent de toutes parts jusqu'à bloquer complètement les systèmes d'information du pays. Mais pourquoi ces sollicitations sont-elles venues simultanément de nombreux pays qui n'avaient rien à voir avec les relations russo-estoniennes ? La technique utilisée fut celle des « botnets », ces ordinateurs ou réseaux d'ordinateurs, situés un peu partout dans le monde, infectés par un virus et devenus zombies. Ils obéissaient à distance aux ordres de serveurs, dits de « Command & Control », commandités, pense-t-on, soit par des groupes autonomes de pirates russophiles, soit par des groupes de pirates contrôlés par l'État russe, le saura-t-on avec assurance un jour ? Ces serveurs « Command & Control » commandaient aux ordinateurs zombies, à l'écoute de leurs ordres, de lancer des sollicitations vers les serveurs Web estoniens. Les botnets, ces armes de perturbation massive, ont ainsi fait du cyberespace un remarquable vecteur de nuisance des états attaqués.

En 2008 éclatait un conflit entre la Russie et la Géorgie, la Russie souhaitant récupérer l'Ossétie du Sud. Suite à des manifestations hostiles de la Géorgie, l'armée russe a pénétré en Ossétie sans que la Géorgie puisse réagir efficacement, car ses systèmes de communication et d'information stratégiques avaient été complètement bloqués au moment de l'attaque russe. De plus, les Web institutionnels géorgiens avaient été défigurés pour donner une image négative du pays assailli. Là, on a vu de vrais tués, pas seulement des cybertués comme dans les jeux vidéo. Ce n'étaient pas, bien sûr, des bits à 0 ou à 1 qui ont tué, ce sont les bombardements, mais les victimes auraient pu être ailleurs si elles avaient pu obtenir les bons renseignements au bon moment. Le monde était entré dans l'aire d'un conflit qui s'appuyait sur la destruction des ressources numériques de l'adversaire, avant de l'abattre.

Cette même année, Conficker, ver particulièrement prolifique, envahissait l'Internet et attaquait les serveurs qui avaient eu la malchance de se trouver sur son passage, en

multipliant les processus dont l'accumulation bloquait leurs capacités de calcul. Beaucoup d'ordinateurs en ont fait les frais. Les aéronefs de certains pays furent bloqués au sol, ou sur leurs plateformes en mer, faute de pouvoir télécharger leurs paramètres de vol. Les réseaux militaires sensibles infectés par le ver Conficker étaient-ils connectés à l'Internet ? Non bien sûr, mais par une clé USB, on transfère facilement un fichier infecté d'un réseau public vers un réseau privé et même confidentiel.

En 2010, il y eut un fait nouveau qui allait populariser un danger auquel tout pays est maintenant exposé : un ver s'attaquait à des infrastructures sensibles très ciblées ! Stuxnet, c'est son nom, fut introduit sur un des serveurs Windows de l'usine d'enrichissement d'uranium de la centrale de Natanz, en Iran. Bien entendu cette infrastructure sensible n'était pas connectée à l'Internet, mais une clé USB ou une barrette mémoire infectée firent l'affaire. Aussitôt le ver se répandit sur les autres serveurs Windows du complexe industriel à la recherche d'un type précis d'automate programmable Siemens connecté au réseau. Ces automates programmables régulaient la vitesse de rotation des centrifugeuses qui servaient à enrichir l'uranium. Un coup Stuxnet faisait tourner les centrifugeuses plus vite, un coup moins vite, un coup elles s'arrêtaient et puis on repartait. Les centrifugeuses ont dû sacrément vibrer et chauffer… Mais les tableaux de contrôle auraient dû s'en apercevoir et sonner l'alarme ! Non, car le ver, qui connaissait les signaux qui étaient envoyés quand tout tournait de façon nominale, les transmettait aux salles de contrôle à la place des vrais signaux d'alerte, pour que les dispositifs de contrôle ne s'inquiètent pas. Bilan : un millier de centrifugeuses détruites et le programme nucléaire iranien arrêté pendant plusieurs mois. Ce ver a popularisé les attaques dites « contre les architectures SCADA (Supervisiory Control and Data Acquisition) ». Avec 4 000 fonctions différentes, l'exploitation de quatre failles non connues, donc sans correctif, dites « failles 0day », utilisant des logiciels signés (par des certificats volés), donc n'éveillant pas la curiosité des défenses des systèmes attaqués, Stuxnet ne pouvait être que créé par une ou plusieurs nations très évoluées et très portées dans la confection de maliciels. Qui était l'agresseur ? Maintenant on le sait, les USA et Israël avaient conçu ce ver très élaboré. Mais suite à un bug, Stuxnet est sorti de l'usine de Natanz dans l'ordinateur d'un chercheur iranien pour parcourir le monde. Il s'est répandu dans de nombreux pays et il a été découvert. Stuxnet ne constitue-t-il pas, là encore, un acte de guerre ? D'autant plus qu'en parallèle à l'attaque de Stuxnet, certains chercheurs iraniens travaillant dans l'industrie nucléaire ont connu une fin tragique.

En 2011, en France, le Ministère de l'Économie et des Finances, ainsi qu'Areva et sans doute beaucoup d'autres entités manipulant des informations très sensibles, ont subi des attaques dites « en APT » (Advanced Persistent Threats). L'attaquant prend connaissance à distance du système d'information et des habitudes des employés de la cible. Au bout de plusieurs mois, par des scans réseaux, par les réseaux sociaux, par des indiscrétions de toutes sortes collectées par téléphone, l'attaquant a constitué une connaissance approfondie de la topologie du réseau cible et des habitudes de ceux qui l'utilisent. Il ne s'agit pas là d'une attaque à l'aveuglette par des virus, les futures victimes sont très ciblées. Un employé, haut fonctionnaire dans le cas de Bercy, reçoit un e-mail provenant d'une origine qui lui inspire confiance (il ne devrait pas). Cet e-mail contient en attachement un fichier, par exemple PDF, à ouvrir de suite. Le PDF ouvert contient le ver qui s'introduit sur son système, capture identifiants et mots de passe, augmente ses privilèges et se répand, par le réseau sur d'autres calculateurs ciblés. Le ver est dans le fruit ! Ensuite, le ver établit un canal de diffusion vers un serveur de « Command & Control » qui va récolter les informations que les postes de travail compromis chiffrent et transmettent. A Bercy, 150 postes de travail ciblés, parmi les plusieurs dizaines de milliers du Ministère, transmettaient ainsi des informations sensibles vers l'étranger (vers la Chine) et cela pendant plusieurs mois. Les secrets du G8 et du G20, dont la France avait la présidence, ont ainsi quitté Bercy. L'ensemble des attaques en APT auraient fait perdre au pays 1% de son PIB. Qu'un pays subtilise les informations sensibles d'un autre pays, nuisant ainsi à sa souveraineté, n'est-ce pas un acte de guerre constitué ?

>>> ARRIVE 2012, ANNEE DE TOUS LES DANGERS.

Ce début d'année a vu le déchainement des Anonymous sur la toile mais on parle là plutôt de cyber hacktivisme, pas de cyberguerre, puisqu'aucun pays en particulier n'était censé être l'agresseur. Parmi les agressés il y eut tout de même en France le site de l'Élysée et ceux de plusieurs ministères. Les Anonymous protestaient contre la fermeture de MegaUpload et contre le fait que les officiels français approuvaient cette fermeture.

Plus en rapport avec notre sujet, en avril 2012, le virus Wiper attaqua les bases de données servant à la gestion portuaire du terminal de Kharg en Iran, seule porte encore ouverte pour exporter leur pétrole malgré les embargos. Des bases de données et de nombreux fichiers indispensables aux échanges commerciaux furent corrompus. Le ver Wiper s'est montré particulièrement

destructeur et les exportations de pétrole iranien ont été bloquées. L'Iran a été encore un peu plus asphyxié par cette agression caractéristique d'une cyberguerre déclarée.

Mais ce n'était pas la dernière cyberattaque qui allait s'abattre sur ce pays, en cette année 2012. Duqu (prononcez Diouquiou), un ver avide en collecte d'informations sensibles, s'est intéressé aux ordinateurs détenus par des personnes ciblées en Iran, au Soudan et dans d'autres pays de la région. Duqu renvoyait les contenus des serveurs piratés à des serveurs de « Command & Control » en Allemagne et au Vietnam. Sitôt découvert, sitôt analysé, Duqu contenait des parties de codes communes avec Stuxnet, le ver qui avait attaqué les centrifugeuses du complexe de Natanz, deux ans auparavant. Mais de là à dire que Duqu était postérieur à Stuxnet, il y a un pas qu'il ne faut pas franchir. Qui connait la date exacte de début de l'agissement d'un maliciel qui peut dormir plusieurs mois avant de se réveiller et agir ?

En juin 2012, le ver Flame fut décelé sur des systèmes d'information de l'Iran et d'autres pays de la région où il sévissait depuis plusieurs années déjà. Cette boîte à outil d'espionnage très sophistiquée, totalisant tout de même vingt mégaoctets de code, installée en tout ou partie sur un poste de travail, écoutait sur les postes de travail infectés, les frappes clavier, faisait des copies d'écran, recherchait des fichiers « Autocad » qui sont en général des plans de lieux stratégiques. Flame parvenait aussi par Bluetooth, à allumer les téléphones portables à proximité des ordinateurs infectés pour écouter les conversations environnantes et même activer leurs caméras. Flame partageait aussi des portions de code avec Stuxnet et Duqu, et utilisait les mêmes vulnérabilités des machines cibles pour se propager. Alors si vous passez par cette région, méfiez-vous de votre Smartphone si vous l'utilisez pour des activités que vous voulez garder pour vous. Votre Smartphone n'est peut-être pas seulement l'objet indispensable pour rester connecté à l'Internet, mais peut devenir un sacré petit bavard et un vilain espion qui relate tous vos actes et paroles, vous qui sans le savoir êtes au beau milieu d'une cyberguerre qui fait rage ! Il ne s'agit pas alors de jouer les héros mais plutôt de vous poser la question « Est-ce cela une bataille ? » comme l'aurait fait un Fabrice Del Dongo dans une Chartreuse de Parme des temps modernes. Et quand Flame fut découvert, il s'est autodétruit, obéissant à une commande venue de l'extérieur. Ainsi cette cyberarme n'a pu être pleinement analysée, et donc reproduite, par les agressés pour répondre aux agresseurs par une autre cyberarme inspirée de la première.

Mais la réponse de l'Iran ne tarda pas à venir avec le virus Mehdi, en juillet 2012, qui s'attaquait à des ordinateurs Israéliens pour leur subtiliser des données sensibles.

Et en cet été 2012, le virus Gauss fit son apparition dans le cyberespace, lui aussi cheval de Troie ultra sophistiqué qui se mit à espionner les ordinateurs des banques libanaises, des banques des territoires palestiniens et bien sûr aussi celles de l'Iran. Était-ce pour déceler des transferts de fond pour l'achat d'armes non conventionnelles par des pays ou des mouvements terroristes ? Là encore nous sommes au cœur d'une cyberguerre. De plus, Gauss peut muter et attaquer les infrastructures sensibles des pays ciblés. A la différence de Flame qui se détruisait sur commande à distance, Gauss se supprimait après trente exécutions. Et quand on constate que Stuxnet, Duqu, Flame et Gauss partagent des portions de code en commun et utilisent parfois les mêmes vulnérabilités des logiciels des ordinateurs cibles pour se propager, on peut émettre des hypothèses sur les auteurs.

Le degré de sophistication et les ressources considérables nécessaires pour le développement de telles cyberarmes, ne peuvent être que le fait de pays. Georges Bush puis Barack Obama ont toujours été favorables à l'utilisation du cyberespace comme théâtre de lutte (opération « Olympic Games ») dont quatre vecteurs (Stuxnet, Duqu, Flame et Gauss), quand ils ont été découverts, étaient en activité depuis déjà plusieurs mois, peut-être depuis plusieurs années. Il faut aussi compter ce qui n'est pas encore découvert et qui est sans doute la partie cachée de l'iceberg.

>>> PEUT-ON GAGNER UNE GUERRE EN LA MENANT SEULEMENT DANS LE CYBERESPACE ?

Je ne pense pas. De même que les bombardements allemands sur la Grande Bretagne en 1940 ou les bombardements des alliés sur l'Allemagne en 1944 n'ont pas suffi à entrainer la reddition de l'adversaire, la destruction des systèmes d'Information et de Télécommunications, et plus généralement la compromission des infrastructures sensibles, peut causer un effet de nuisance extrême sur un pays mais ne peut le contraindre pour autant à se soumettre à la volonté du vainqueur. Pour vaincre, si tel est le but, une agression physique dans le périmètre terre/air/mer/espace doit suivre les effets obtenus par le cyberespace.

>>> LA CYBERGUERRE PEUT-ELLE CONSTITUER UN ETAT DE GUERRE ?

La question mérite d'être débattue. Il est sûr que si une guerre implique l'usage de la force, tant qu'on reste dans le

numérique, les dégâts sont visibles mais où est « la force » ? La cyberguerre est plutôt assimilable à ce qui se passait durant la guerre froide. Des escarmouches, un espionnage exacerbé de tous les côtés, mais pas d'invasion brutale du territoire adverse. On possède des armes de destruction massive mais on ne les utilise pas, par peur des représailles. Certes la destruction de l'infrastructure électrique d'un pays paralyserait totalement le pays agressé. Et plus le pays est évolué, plus il a à craindre une telle éventualité, surtout les pays qui, par l'Internet, régulent l'offre en énergie avec la demande des foyers, comme aux États-Unis avec les Smart Grids. Mais qui franchirait la ligne rouge au risque de déclencher les foudres de l'adversaire, et pas seulement dans le cyberespace, et pas seulement avec des armes virtuelles ?

Le risque est donc accru depuis qu'aux champs de bataille classiques s'est ajouté le cyberespace. Plus que jamais, et l'année 2012 le justifie, entre paranoïa collective et insouciance, mieux vaut renforcer la cybersécurité au niveau de toutes les infrastructures vitales d'un pays et se tenir au courant du développement des cyberguerres qui font rage dans le cyberespace.

>>> A PROPOS DE L'AUTEUR

Gérard Peliks est expert sécurité chez Cassidian CyberSecurity. Cassidian est la division « Defense and Security » d'EADS, Cassidian CyberSecurity regroupe les activités « cyberdéfense » de Cassidian.

Il préside l'atelier sécurité de l'association Forum ATENA, et coordonne l'activité sécurité de l'Information du Cercle d'Intelligence Économique du Medef Île-de-France.

Il est chargé de cours sur différentes facettes de la sécurité, dans le cadre de mastères à Telecom ParisTech et dans d'autres écoles d'Ingénieurs. A l'ISEP, il intervient sur des modules sécurité dans le cadre des mastères spécialisés et a participé au comité de pilotage du Mastère Spécialisé en Intelligence des Risques et des Opportunités par l'Intelligence Économique.

La formation continue à l'ISEP

Par Denis Beautier
Professeur d'Informatique à l'ISEP
Directeur des Formations Continues de l'ISEP

Pour son activité Formation Continue, l'ISEP a choisi une stratégie de niche et de pionnier. Aux côtés de la formation initiale des ingénieurs, qui constitue son cœur de métier, de la recherche et des relations internationales, l'ISEP propose depuis déjà plus de trente ans une offre de Formation Continue qui permet aux professionnels de maintenir et d'améliorer leur employabilité tout au long de leur vie.

L'activité Formation Continue de l'ISEP[1] forme aujourd'hui des experts dans des domaines innovants où les compétences sont rares et recherchées.

>>> INFORMATIQUE & LIBERTES

C'est en 2004, avec la révision de la loi Informatique et Libertés, qu'ISEP Formation Continue a identifié le premier métier qui correspondait à cette nouvelle stratégie : le Délégué à la Protection des Données Personnelles, mieux connu sous l'appellation de CIL pour Correspondant Informatique et Libertés. Il s'agissait alors d'une fonction expérimentale, initiative soutenue alors par le Président de la CNIL, Monsieur Alex Türk. Les objectifs de ce nouveau métier sont de protéger les données personnelles et à travers elles la vie privée des personnes concernées (salariés, clients, prospects, patients, administrés, etc.). La fonction a été encadrée par un décret en octobre 2005 et Pôle Emploi a créé le code ROME en décembre 2011. Chaque responsable d'entreprise, de collectivité, d'établissement de soins, d'école a la faculté de désigner un CIL auprès de la CNIL, et dix mille d'entre eux ont fait ce choix, dont plus de la moitié des grandes entreprises. Le CIL est un facteur d'autorégulation et un vecteur de sécurité juridique par réduction des risques légaux, opérationnels, financiers et d'image.

C'est la formule du **Mastère Spécialisé** qui a été retenue. Il s'agit d'un label créé en 1983 par la CGE (Conférence des Grandes Écoles) pour répondre à une demande des entreprises françaises qui souhaitaient recruter des diplômés possédant des compétences dans des spécialisations très pointues. L'admission se fait aux niveaux BAC+5 et BAC+4 avec expérience.

Des demandes d'agrément ont toutefois été déposées également pour pouvoir proposer des B.A.D.G.E (Bilans d'Aptitudes Délivrés par les Grandes Écoles) et intégrer dans les promotions des candidats présentant un profil BAC+2 avec expérience dans le cadre du régime dérogatoire.

La conception du contenu de la formation s'est avérée passionnante, car il s'est agi d'une pure création. Dès 2004, l'ISEP s'est rapprochée de la CNIL (Commission Nationale Informatique et des Libertés) et de l'AFCDP (Association Française des Correspondants à la protection des Données Personnelles). Une convention a été établie avec cette dernière et un groupe de travail réunissant les professionnels concernés a dessiné les grandes lignes du cursus autour de quatre axes : juridique, technique, métier et sectoriel.

L'une des grandes inconnues était de savoir s'il serait possible de regrouper dans une seule et même promotion des profils aussi divers que des juristes d'entreprise, des informaticiens, des qualiticiens, des documentalistes-archivistes, des auditeurs… Certains prônaient l'organisation de parcours préalables de mise à niveau avant de regrouper les candidats dans un tronc commun. C'est finalement la première option qui a été retenue pour l'ouverture en 2007. Immédiatement cette « mixité » est apparue comme une formidable richesse, le métier de CIL étant éminemment transverse.

Le passage devant le jury d'admission est un moment clef.

[1] *www.FormationContinue-ISEP.fr*

Au-delà de son objectif principal – vérifier que l'obtention du grade de Mastère Spécialisé est bien l'un des facteurs qui permet d'atteindre l'objectif présenté dans le cadre du projet professionnel du candidat – une grande attention est portée à la démarche éthique. S'agissant de la protection de la vie privée des personnes, l'école ne souhaite pas former des « experts désincarnés », capables de réciter des articles de loi intégralement, sans se sentir « habités » par la fonction. Rappelons que la loi Informatique et Libertés se fonde sur la primauté de la personne : comme le dit son article premier : *« L'informatique doit être au service de chaque citoyen […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques»*.

Un grand soin a également été porté sur la sélection des intervenants, ce Mastère Spécialisé étant présenté comme une formation des CIL par d'autres CIL. Aux côtés de Correspondants Informatique et Libertés de grandes entreprises (RATP, CNP Assurances, Casino, Banque de France, etc.) figurent plusieurs avocats spécialisés, des agents de la CNIL et des experts étrangers (il faut savoir que, par exemple, la CNIL espagnole inflige annuellement plus de vingt millions d'euros de sanctions financières). Les professionnels sont également régulièrement invités à prendre part aux différents jurys, qu'ils soient d'admission, de projets transversaux ou de thèses professionnelles.

ISEP Formation Continue a ouvert en octobre 2012 la 6ème promotion de ce Mastère Spécialisé[1] « Informatique et Libertés » et y apporte des améliorations de façon continue. Un service de soutien a été introduit en 2010 pour épauler les apprenants dans leur projet de thèse professionnel, afin que celles-ci répondent aux attentes de la communauté des professionnels concernés. Plusieurs d'entre elles ont d'ailleurs été saluées par la Presse et une sélection est adressée chaque année au Président de la CNIL.

Les diplômés sont recherchés et nombreux sont les organismes qui proposent d'accueillir un apprenant afin que celui-ci effectue sa mission en entreprise : à l'issue de celui-ci, ils peuvent ainsi bénéficier d'un audit de conformité, d'un plan de progrès, d'un inventaire des traitements de données personnelles opérés au sein des différentes directions métier, d'une évaluation des risques.

Le contenu évolue également en fonction des décisions de jurisprudence, des publications des différentes autorités de contrôle, des évolutions technologiques : de nouveaux modules ont été ajoutés pour se préparer au futur règlement européen, dont le projet a été publié le 25 janvier 2012 par la Commission européenne. Outre une très nette augmentation des risques pour les entreprises (les sanctions financières pourront aller jusqu'à 2% du chiffre d'affaires mondial), de nouvelles exigences apparaissent, comme celle qui obligera à informer chaque client d'une violation de ses données personnelles, comme cela se pratique depuis plusieurs années aux États-Unis.

Le projet de règlement européen – qui s'appliquera donc directement aux états Membres dès sa promulgation – prévoit également de rendre obligatoire le « Délégué à la protection des données », et certains prévoient déjà une pénurie de professionnels formés. Cette filière est donc promise à un grand avenir.

Un éventail de formations courtes, d'un à trois jours, sont également proposées sur ce même thème, comme celle qui permet d'apprendre à piloter un projet d'anonymisation de données personnelles – pour éviter que les développeurs ne travaillent sur une copie des données de production – ou ce module de deux jours qui permet à des juristes d'entreprise d'interagir avec des informaticiens.

>>> CLOUD COMPUTING & SaaS

Plus récemment, ISEP Formation Continue a fait évoluer en profondeur un second Mastère Spécialisé qui avait été créé sur une demande initiale de France Telecom, qui souhaitait faire évoluer ses personnels et leur permettre notamment de gérer des portefeuilles de projets. Ce cursus était connu sous l'appellation de VAMOS (pour Value Added Media Operational Services).

A la suite d'une analyse des attentes du marché, il a été décidé d'en conserver l'esprit *(« la technique c'est bien, mais il n'y a pas que ça dans la vie »)* pour former les experts du Cloud Computing et du SaaS[2].

Le Cloud Computing ne fait pas que modifier la façon de consommer l'informatique, il change aussi les métiers au sein des directions informatiques. Bien que l'informatique dématérialisée ne s'appuie pas sur des avancées technologiques, elle n'a rien d'un effet de mode ni d'une simple évolution. Quelle que soit la façon de considérer le phénomène, de nouvelles problématiques voient le jour, comme la maîtrise des cycles de vie d'une instance, l'impact de la qualité du code sur le niveau de facturation, les règles de gouvernance ou la logique de tarification. D'autres questions doivent être revisitées, comme la souveraineté, la sécurité, la confidentialité, la traçabilité, la conformité aux

[1] *www.Informatique-et-Libertes-Formation.fr*
[2] *Software as a Service*

lois concernant la protection des données personnelles et la réversibilité/transférabilité des contrats.

Avec le Cloud Computing, on peut dire que l'ère de l'artisanat en matière d'informatique touche à sa fin et, qu'une nouvelle fois, les métiers de la DSI changent… moins techniques, ils deviennent toujours plus fonctionnels et orientés vers le business des entreprises. Il est donc indispensable que les collaborateurs à qui sont confiés ces sujets bénéficient de formations adéquates : les entreprises doivent acquérir le niveau de compétences qui leur permettra de concevoir l'expression de besoins idéale, de « challenger » les offreurs de service, de réaliser une maîtrise d'œuvre de haute tenue, de prononcer une recette en connaissance de cause. Comme l'externalisation, le Cloud Computing a sa règle d'or : « garder le cerveau et sous-traiter les jambes ». De plus, afin d'anticiper l'éventuel reclassement des personnels informaticiens qui ne répondent plus à ces nouvelles exigences, les directions des ressources humaines doivent étudier les démarches d'accompagnement indispensables.

Une nouvelle labélisation a donc été obtenue auprès de la CGE pour ce nouveau cursus, dont la première promotion a ouvert en octobre 2012.

Outre un axe technique, le Mastère Spécialisé[1] « Expert Cloud Computing et SaaS » comprend une composante d'ouverture transverse qui couvre les aspects juridiques, contractuels, financiers et commerciaux, mais également la prise en compte de la satisfaction client, la gestion des équipes et des sous-traitants, les relations avec le marketing.

Les candidats doivent soutenir une thèse professionnelle, réflexion personnelle sujet de son choix avec prise de hauteur. Voici quelques exemples de sujets : Quelles précautions contractuelles prendre pour assurer une réversibilité ou une transférabilité idéale dans le cadre d'un projet IaaS[2] ? Gérer la conduite du changement dans la cadre d'un projet Cloud Computing, Chiffrement et Cloud Computing : Mythes et légendes, Réussir une migration vers IPv6, etc.

Certains modules de ce Mastère seront sans doute prochainement déclinés en formations courtes, comme celui consacré au Modèle Économique. Tous les aspects économiques des contrats Cloud Computing y sont déchiffrés, aussi bien du point de vue du client que de celui de l'offreur : Répartition des investissements dans la chaine de valeur, impact pour le fournisseur (cashFlow, étalement dans le temps, développement initial, valorisation, durée d'engagement minimale, …), facturation et raréfaction des services dynamiques, différents modes de facturation (per User, per Ressource, per Transaction), les différentes tactiques de prix (no cost, freemium, crédits, etc.), les éléments exogènes (taxes, risques et couverture de change, etc.), la gestion des refacturations internes ou des ventilations budgétaires, la préparation des budgets, la coopération entre Service Achats et Chef de projet Cloud.

Dans le cadre du partenariat établi à l'occasion avec le CSA (Cloud Security Alliance), les apprenants pourront tenter de décrocher en sus la certification sécurité Cloud que propose cette association. D'autres partenariats existent pour consolider les liens avec les besoins du marché : EuroCloud, Oracle, …

Il faut noter que, pour les deux Mastères spécialisés que propose actuellement l'ISEP, le calendrier des formations a spécialement été conçu pour permettre à des professionnels de tenir leur poste.

>>> AUTRES FORMATIONS

La Formation Continue de l'ISEP est aussi contactée pour répondre à tout type de besoin de formations sur mesure dans les domaines exposés ci-dessus, mais aussi dans tous les domaines des Technologies de l'Information et de la Communication et du management de ces technologies. Par exemple, la formation continue a déjà formé dans ce contexte les chefs de projets du Ministère de l'Intérieur. Depuis 2009, quatre promotions se sont succédé et 60 élèves ingénieurs ont été formés. Ce cursus a aussi été monté en partenariat avec un cabinet de conseil spécialisé : ACDE-Conseil. Il s'agit d'un cursus de la même ampleur que les deux Mastères Spécialisés ci-dessus.

La formation continue a également été sollicitée il y a peu pour former sur quelques semaines une équipe de développeur qui migrait de .Net à Java.

>>> STRATEGIE

Cette stratégie de niche et de pionnier s'adresse tout naturellement à tous les professionnels, notamment aux anciens élèves de l'ISEP, qui peuvent y trouver les solutions à leurs besoins, tant pour se former eux-mêmes que former leurs équipes, voire faire connaître l'offre de l'ISEP à leurs collaborateurs (des partenariats riches sont en effet possibles sur ces sujets). Ils peuvent aussi formuler leurs besoins de profils, tant pour des missions opérationnelles dans le cadre des stages des mastères spécialisés qu'à l'embauche en fin

[1] *www.Cloud-Computing-Formation.fr*
[2] *Infrastructure as a Service*

de formation. Ils peuvent aussi se proposer comme intervenants, voire découvrir nos solutions en souhaitant participer aux jurys de sélection des candidats, aux jurys des projets transversaux et aussi aux jurys des thèses professionnelles.

La formation continue de l'ISEP est un lieu d'excellence où se rencontrent des experts à forte valeur ajoutée et à très fort potentiel entreprenarial.

>>> PETIT RETOUR EN ARRIERE

La Formation Continue de l'ISEP tire sa force de son histoire. Tout a commencé à l'initiative d'un homme, un ancien ISEP, que beaucoup connaissent, Jean-Pierre Jourdan [ISEP 65], toujours en étroite collaboration avec les Directeurs successifs.

L'aventure a commencé en 1982 par la création d'une « année spéciale » dans le cadre du plan de rattrapage de la filière électronique des pouvoirs publics, afin de repositionner des ingénieurs dans cette spécialité en demande de profils en leur délivrant un deuxième diplôme répondant aux critères de la Commission des Titres d'Ingénieurs (CTI). Deux promotions ont permis de former 67 ingénieurs pour les repositionner de secteurs économiques en difficulté vers un secteur porteur en forte demande. Cette histoire s'est terminée par la fin des subventions accordées par les pouvoirs publics.

Forte de cette expérience, la formation continue a décliné sur le marché des sessions courtes interentreprises de un à cinq jours, pour maintenir à niveau les ingénieurs sur ces techniques mais aussi pour les étendre à celles de l'informatique. Ces sessions ont pu vivre grâce à la nouvelle taxe de formation obligatoire créée à cet effet.

En 1990, ces deux expériences ont jeté les bases d'un partenariat avec Thomson autour d'un cursus intra-entreprise d'*exploitant réseaux hétérogènes* pour certains de ses techniciens ayant au moins trois années d'expérience. Celui-ci s'est déroulé tant à l'ISEP qu'au Campus Thomson, sur une durée de 600 heures.

En parallèle, un nouveau besoin est apparu, dans cadre du rapport Decomps, où l'État devait trouver des solutions pour former davantage d'ingénieurs et assurer la promotion en ingénieurs, après 1750 heures de formation sur trois années, de techniciens ayant au moins cinq années d'expérience. La formation se déroulait à l'ISEP en alternance, le vendredi et le samedi matin. L'ISEP s'est alors doté d'un deuxième diplôme d'ingénieur reconnu par la Commission des Titres d'Ingénieurs (CTI), pour marquer sans confusion possible la différence avec son diplôme d'ingénieur de formation initiale. L'ISEP a proposé de former dans son cœur de métier, des ingénieurs « temps-réel ». C'est dans ce contexte qu'a spécialement été créée en 1990 l'association « Institut Supérieur des Techniques d'Électronique de Paris » (ISTEP) et la SARL ISEP Formation Continue. Thomson ayant arrêté son cursus intra-entreprise d'exploitant réseaux hétérogènes après cinq promotions, il a été décidé d'ajouter une option « réseaux » au cursus d'ingénieur par la formation continue, pour former les publics des autres entreprises dans cette spécialité. Par la suite cette filière Décomps a été rebaptisée Nouvelle Formation d'Ingénieur (NFI), puis Formation d'Ingénieur en Partenariat (FIP). Elle s'est naturellement arrêtée en 2005 par le tarissement des techniciens à former, suivi par celui des financements de l'État, après 14 promotions et 320 diplômés.

L'ISEP venait d'ouvrir des Masters of Sciences de la Conférence des Grandes Écoles (CGE) dans le cadre de ses formations internationales. La Formation Continue a donc senti qu'elle pouvait proposer des Mastères Spécialisés de la CGE, d'une durée de l'ordre de 350 heures et qui s'adresseraient principalement à des ingénieurs. Ils peuvent aussi être découpés en deux Bilans d'Aptitude Délivré par les Grandes Écoles (BADGE) de 250 heures chacun, dotés d'un tronc commun, pour permettre aux meilleurs techniciens d'accéder au label prestigieux par un système dérogatoire contrôlé. Il s'agit d'un ensemble de formations souples, haut de gamme et spécialisées, adaptées aux réalités du marché.

Il a notamment été créé le Mastère Spécialisé en « Intelligences des Risques et Opportunités par l'Intelligence Économique ». En ces temps de crise, l'idée était de proposer une formation autour de la gestion de l'information pour gérer les risques mais aussi identifier des opportunités. Cette très riche expérience a été le fruit de belles rencontres avec un ancien élève, Jean-Marc Beignon [ISEP 75] et deux experts de renom, Bernard Besson et Jean-Claude Possin. Une promotion de grande qualité a été formée. La formation n'a pas été reconduite pour concentrer l'offre des formations sur le cœur de métier de l'ISEP et intégrer les paramètres de la crise économique. Aujourd'hui, les MS et BADGE existants sont dans les domaines « informatique et libertés » et « Cloud Computing ». Une « intra » du même ordre existe dans le domaine du « management de projet informatique ».

La Formation Continue est donc une aventure qui tire aujourd'hui sa force d'un passé riche de formation tout au long de la vie, d'écoute des besoins du marché, d'un positionnement sur des sessions courtes et des cursus inter-entreprise, mais aussi intra-entreprise, sur mesure. Ce sont aussi des partenariats avec des acteurs du marché et des rencontres humaines.

L'ISEP Formation Continue doit rester souple et savoir s'adapter à son environnement.

Aujourd'hui, choix a donc été fait, non pas de se positionner en concurrence avec d'autres établissements nombreux à proposer des formations sur des thématiques identiques, mais au contraire de se démarquer en se focalisant sur des métiers nouveaux, dont l'esprit répond à l'approche humaniste de l'ISEP. Cela ne l'empêche pas de répondre avec justesse et un souci d'excellence à des besoins plus classiques.

Contact : Denis Beautier - Directeur des formations continues

denis.beautier@isep.fr - 01 49 54 52 20

>>> A PROPOS DE L'AUTEUR

Denis Beautier est titulaire d'un DEA Informatique, Réseaux et Systèmes Embarqués (1989). Il a commencé son expérience dans la formation comme Volontaire Formateur en Informatique dans le cadre de son Service National, puis comme ingénieur dans l'armement chez Thalès durant 5 ans.

Il est ensuite retourné à ses amours premières pour former des collègues avec un souci de l'excellence technique, managériale mais aussi humaine, comme consultant formateur durant deux ans, puis professeur d'informatique en école d'ingénieur durant cinq ans, avant de rejoindre l'ISEP en 2001.

A l'ISEP, il enseigne et prend la responsabilité des ISTEP, et fait évoluer la Formation Continue avec notamment la création des Mastères Spécialisés. Il est aujourd'hui Professeur d'Informatique à l'ISEP et Directeur des Formations Continues de l'ISEP

Témoignage

Par Stéphane Degryse
Titulaire du Mastère Spécialisé en Intelligence des Risques et des Opportunités par l'Intelligence Économique de l'ISEP
Délégué Défense et Sécurité
Agence Nationale de Sécurité du Médicament et des produits de santé

>>> EXISTE-T-IL UN MODELE D'INTELLIGENCE ECONOMIQUE APPLICABLE AU MONDE ASSOCIATIF ?

En 2008, 15,8 millions de Français étaient membres au moins d'une association, soit près d'un tiers des Français de plus de 16 ans, selon l'étude publiée par l'INSEE. C'est donc tout à fait naturellement que je me suis intéressé dès le départ à ce monde vaste de richesses individuelles, mais sur lequel finalement assez peu d'écrits étaient disponibles.

Et c'est en partie grâce à une connexion via le réseau social Viadéo, que j'ai été amené à rencontrer en juillet 2010 les membres de l'association HéxaVeiL. Monsieur Didier Ronté, nouvellement élu Président de cette association, m'a d'emblée proposé de travailler au sein de l'association dans le cadre du Mastère Management des risques et intelligence économique de l'ISEP. J'ai donc intégré officiellement l'association dès le 1er septembre 2010.

L'association HéxaVeiL, est une association nantaise dont la vocation est de réfléchir à des solutions globales en matière de sécurité publique. Cette réflexion est menée de concert par tous les membres de l'association (police, gendarmerie, industriels, commerciaux et citoyens). La volonté de l'association est également d'associer les élus à sa démarche afin de proposer des solutions adaptées, applicables et dont le déploiement est en corrélation avec les problématiques en matière de sécurité publique. Les cibles visées sont les communes et les communautés de communes.

A partir de ces données fondatrices qui m'ont attirées, j'ai demandé à son Président, Monsieur Didier Ronté, s'il était favorable à ce que j'effectue mon stage de thèse professionnelle dans cette association.

Grâce à son accord et avec l'appui sans faille de Monsieur Roman Regas, j'ai proposé de mettre au point une stratégie associative de recherche d'informations dans le cadre d'un système d'intelligence économique. Il est calqué en tous points sur le modèle de Système d'Intelligence Économique d'Entreprise tel qu'il est défini par Messieurs Bernard Besson et Jean-Claude Possin dans leur livre, De l'intelligence des risques à la mission de protection, IFIE édition. Je me suis également inspiré des cours reçus en cette année 2010/2011 par tous les intervenants de l'Institut Supérieur d'Électronique de Paris dans le cadre du Mastère Spécialisé « Management des risques et des opportunités par l'intelligence économique ». Bien que le nombre d'écrits sur le développement économique associatif soit très faible, j'ai néanmoins réussi à mettre en œuvre une méthode de l'intelligence économique, permettant le développement de l'association. Ce développement est fondé sur les 4 piliers – mémoire, maîtrise, réseaux, analyse – qui reposent sur une logique de recherche d'informations.

Bibliographie des auteurs

BERNARD BESSON ET JEAN-CLAUDE POSSIN

- Du renseignement à l'intelligence économique Cybercriminalité, contrefaçon, veilles stratégiques : détecter les menaces et les opportunités pour l'entreprise. Dunod seconde édition mai 2001,
- L'audit d'intelligence économique Mettre en place et optimiser un dispositif coordonné d'intelligence collective Dunod 2ème édition août 2002
- l'Intelligence des risques Intelligence économique, Sécurité, sûreté, environnement, management. L'intelligence économique pour prévenir les crises au lieu de les gérer. Editons IFIE (Institut Français d'intelligence économique) collection « pratique de l'IE » janvier 2006.
- Intelligence économique et gouvernance compétitive ouvrage collectif du groupe IE de l'INHES, Documentation Française à paraître premier semestre 2006.
- De l'intelligence des risques à la mission de protection tome 1 : - du concept au système, tome 2 : - pratique de la mission protection-sécurité- IFIE Octobre 2008.
- Retour sur investissement (RSI) en intelligence économique et valorisation du capital immatériel Encyclopédie Weka « Management stratégique de l'information » juin 2010.
- L'Intelligence Inventive Bernard Besson et Renaud Uhl Rie N° 29 et 30 de juin 2010
- Des Neurosciences au management décisionnel par l'IE Jean-Claude Possin et Docteur R. Caltabellotta Rie N° 30 juin 2010.
- Intelligence décisionnelle et sciences cognitives Sciences cognitives, Neurosciences et processus de décision. J-C Possin et R. Caltabellotta éditions IFIE sortie prévue fin 2012.

PATRICE KAHN

- Anticipation, innovation, perception : des défis pour la maîtrise des risques à l'horizon 2020 Patrice Khan, André Lannoy, Dominique Person-Silhol, Dominique Vasseur. Tec & Doc collection Sciences du risque et du danger.

BRUNO RASLE

- Halte au Spam et Frédéric Aoun, Bruno Rasle. Eyrolles 2003

Communiqué : une seconde session pour le Master spécialisé : « Experts Cloud Computing »

L'ISEP décide d'ouvrir une seconde session de son Mastère Spécialisé pour former les Experts du Cloud Computing et du SaaS.

Après avoir ouvert en octobre la première session de son nouveau cursus diplômant destiné à former les experts de l'infonuagique, la grande école décide d'ouvrir une seconde session, décalée, afin de répondre aux nombreuses demandes.

6 novembre 2012 – La grande école ISEP (Institut Supérieur d'Electronique de Paris) a conçu un cursus diplômant (en temps partiel) pour répondre à la pénurie de spécialistes de l'infonuagique, car le Cloud Computing ne fait pas que modifier la façon de consommer l'informatique, **il change aussi les métiers au sein des directions informatiques** et réclame de nouvelles compétences.

La rentrée de la toute première promotion 2012-2013 du Mastère Spécialisé « Expert Cloud Computing et SaaS » s'est déroulée 18 octobre 2012.

La promotion, sous l'œil bienveillant d'Edouard Branly, découvreur des principes de la radio conduction et de la télémécanique, pionnier de la radio (1844-1940)

D'emblée, les participants se montrent enthousiastes : « On se rend compte des moyens humains conséquents et riches mis à notre disposition par l'ISEP », *« Très bon retour d'expériences et approche globale sur les processus métiers intéressants », « Exceptionnel. Je n'ai tout simplement jamais assisté à un cours de cette qualité-là », « L'intervenant nous fait partager son impressionnante expérience et sa vision du futur du Cloud Computing », « Passionné et captivant, L'intervenant nous régale »…*

La labélisation par la Conférence des Grandes Ecoles n'étant intervenue qu'en avril, nombreuses ont été les professionnels intéressées à rejoindre ce cursus n'ayant pas eu le temps de finaliser leur projet professionnel.

Aussi, afin de leur éviter d'attendre la rentrée d'octobre 2013, **la grande école ISEP a donc décidé d'ouvrir une nouvelle session, en mars 2013**. Les cours se tiendront donc jusqu'en décembre 2013, avec une soutenance de thèse professionnelle en 2014.

Ce cursus est destiné aux ingénieurs et techniciens - Télécom, Réseaux ou Informatique – qui souhaitent donner un coup d'accélérateur à leur carrière en s'appuyant sur leurs compétences techniques, ou à se reconvertir pour profiter de la « vague » du Cloud Computing au lieu de la subir.

Cette formation comporte **deux axes**. **L'un, technique**, permet d'acquérir et de consolider les connaissances technologiques spécifiques à l'environnement Cloud Computing. **Le second, transversal**, assure l'ouverture sur toutes les autres facettes indispensables à la réussite des projets (aspects légaux et règlementaires, aspects financiers et fiscaux, relations avec le marketing, gestion d'équipes et de crises, prise en compte de la satisfaction clients, gestion des partenariats et de la sous-traitance, maîtrise des aspects contractuels, gestion de la réversibilité/transférabilité, etc.).

« Nous en profitons pour enrichir les contenus. Ainsi nous venons d'ajouter l'étude des impacts fiscaux sur un basculement en mode SaaS » indique Denis Beautier, Responsable du programme, qui ajoute « L'ouverture de la première promotion nous a également donné l'occasion d'entrer en contact avec de nouveaux experts et professionnels en activité, qui feront part de leur expériences, bonnes ou…moins bonnes auprès de nos participants ».

Voici deux exemples de modules très spécifiques à ce Mastère Spécialisé :

Gestion du sourcing : Nul doute **qu'il y aura des « morts » dans les années à venir parmi les acteurs qui se proclament aujourd'hui « leader » sur ce marché**. Il convient donc de sélectionner avec soin son prestataire. Un module met en scène une entreprise qui cherche à migrer vers le Cloud Computing et à sélectionner le partenaire adéquat. Une moitié de la promotion joue le rôle du client (expression de besoins, formalisation des exigences, préparation des budgets, méthode de sélection des offres, points contractuels, procédure de recette, suivi des engagements de sécurité, de QoS et de disponibilité , vérification de la facturation, préparation à un éventuel transfert ou réversibilité, etc.), tandis que l'autre moitié jour le rôle de l'offreur (réponse aux questions, présentation argumentée de l'offre, objectivation des engagements, etc.).

Tarification, facturation et business model : Un éditeur de logiciel qui bascule d'un modèle de facturation de type licence à un modèle SaaS doit concevoir une nouvelle logique de tarification qui puisse assurer son développement tout en restant compétitif. De l'autre côté, les entreprises clients doivent pouvoir s'assurer que les économies promises à court terme seront au rendez-vous, mais qu'elles ne seront pas obérées par une explosion de la facturation les années suivantes ! Comment disposer d'une visibilité/prédictibilité sur la facturation en mode SaaS ? Comment vérifier que le montant facturé correspond à une réalité ? Comment tenir compte des effets de bord fiscaux ?

Fiche d'identité du Mastère Spécialisé « Expert Cloud Computing et SaaS »

Label de la Conférence des Grandes Ecoles
Cours en présentiel, sur une année universitaire (ou deux ans)
Deux rentrées par an (mars et octobre)
En temps partiel (permettant d'exercer son activité en parallèle), 350 heures (45 jours)
Trois projets transversaux à réaliser
Une mission en entreprise à effectuer
Une thèse professionnelle à soutenir
Admission BAC+5 et BAC+4 avec expérience
Régime dérogatoire à partir de BAC+2
Intervenants professionnels et experts
Prise directe avec le marché
Partenariat avec Eurocloud France, CSA, Microsoft, France Telecom, Thales, Oracle, etc.
Accompagnement personnalisé
9.950 € HT

Site Web : www.cloud-computing-formation.fr

Contact : Denis Beautier, Directeur des Formations Continues ISEP
Tel. 01 49 54 52 20 et 06 73 11 74 02 – denis.beautier@isep.fr

A propos de l'ISEP : www.isep.fr *Situé au cœur de Paris, l'ISEP est reconnu comme faisant partie des meilleures écoles d'ingénieurs françaises. L'ISEP dispense une pédagogie innovante, qui intègre la pédagogie par projet et l'approche par compétence. L'école forme chaque année plus de 180 ingénieurs généralistes en technologies de l'information et de la communication. Il propose son cursus en apprentissage depuis 1996 mais également 2 Mastères Spécialisés (Informatique et Libertés, Cloud Computing) et 4 B.A.D.G.E. Les ingénieurs de l'ISEP se retrouvent dans les secteurs industriels, des services, des banques, etc. La Junior Entreprise de l'ISEP, JUNIOR ISEP, fleuron associatif de l'esprit entrepreneurial est aujourd'hui la meilleure Junior entreprise ingénieur française (Prix d'Excellence 2005 et 2008, finaliste 2009)*