cigref
Réseau
de Grandes Entreprises

PROMOUVOIR LA CULTURE NUMÉRIQUE
COMME SOURCE D'INNOVATION ET DE PERFORMANCE

Les risques numériques pour l'entreprise

mars 2011

Le CIGREF, réseau de Grandes Entreprises, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...). Le CIGREF a pour mission de promouvoir la culture numérique comme source d'innovation et de performance.

Titre du rapport : Les risques numériques pour l'entreprise

Equipe du CIGREF

Jean-François Pépin - Délégué Général
Sophie Bouteiller - Chargée de mission
Marie-Pierre Lacroix – Chef de projet
Josette Leman - Assistante de direction
Frédéric Lau - Directeur de mission
Anne-Sophie Boisard - Chargée de recherche
Armand François : Assistant de recherche
Josette Watrinel - Secrétaire de direction

Remerciements :

Nos remerciements vont à Kyomi ARRACHEA, Stéphane BOUCHE OSOCHOWSKI et Youssef LAKHIRY, Étudiants en master Management des Risques Internationaux à HEC qui ont conduit ce travail durant leur stage au CIGREF.

Nous remercions également les personnes qui ont participé à cette étude :

- Mme Elisabeth HUMBERT BOTTIN, GIP MDS
- M. Nicolas BOURGEOIS, Juriste Auchan
- M. Hubert TOURNIER, Adjoint du DOSI et Directeur conseil Mousquetaires
- M. Gregor MACIAK, Consultant Osiatis
- M. Georges Edouard DIAS, Directeur Web Marketing L'Oréal
- M. Arnaud LACAZE, Chargé de mission DGME

Pour tout renseignement concernant ce rapport, vous pouvez contacter le CIGREF aux coordonnées ci-dessous :

CIGREF
21, avenue de Messine 75008 Paris
Tél. : + 33.1.56.59.70.00
Courriel : contact@cigref.fr

Sites internet :
http://www.cigref.fr/
http://www.fondation-cigref.org/
http://www.histoire-cigref.org/
http://www.collection-cigref.org/
http://www.entreprises-et-cultures-numeriques.org/

SYNTHÈSE

Il existe un nombre important de risques dont les conséquences s'appliquent à des domaines très différents dans l'entreprise : les métiers, les relations avec les parties prenantes…

Les risques liés au numérique sont ceux qui surviennent lors du « passage » au numérique ainsi que ceux à gérer tout au long de la vie de l'entreprise. Ils ne sont pas circonscrits au seul périmètre des systèmes d'information et sont transversaux puisque le numérique est au cœur de la chaine de valeur de l'entreprise.

L'entreprise numérique peut se définir comme « *une entreprise qui tire une part de sa valeur de la numérisation de ses activités, ses produits ou ses clients.* ». Le risque, lui, peut se définir comme la conjonction d'un aléa et d'un enjeu.

Dans ce cadre, nous avons identifié 31 risques liés au numérique regroupés en huit familles :

1. Les risques liés aux ressources humaines ;
2. Les risques liés à la dématérialisation des rapports humains ;
3. Les risques stratégiques ;
4. Les risques liés au contrôle des systèmes d'information ;
5. Les risques éthiques et juridiques ;
6. Les risques liés au patrimoine numérique ;
7. Les risques marketing ;
8. Les risques périphériques.

Tous ces risques peuvent être mesurés en fonction d'un degré d'occurrence et d'un degré de gravité dont la combinaison détermine le facteur de risque pour l'entreprise. A partir de ces éléments, l'établissement d'une cartographie statistique des risques permet de mettre en lumière plusieurs points :

Des risques SI maîtrisés

Le facteur de risque lié au contrôle et à la maitrise du système d'information, risque auquel on pense de prime abord lorsqu'on évoque l'entreprise numérique, apparait comme étant relativement peu important. Ces risques, parce que bien connus, sont généralement bien maitrisés, et leur impact est donc faible sur la vie de l'entreprise.

Un risque majeur : le manque de culture numérique

Les principales sources de danger sont plus liées au manque de culture numérique des dirigeants comme des salariés de l'entreprise. Un défaut de stratégie numérique, une mauvaise

gestion des ressources humaines lors du « passage » au numérique ou des problèmes liés à la dématérialisation des rapports humains sont autant de risques majeurs qui peuvent entrainer d'importants dommages pour l'entreprise.

D'une stratégie numérique indispensable…

Une stratégie numérique apparait à la fois comme un outil de prévention mais aussi comme un important facteur de risque. Sa défaillance peut entrainer la survenance d'autres risques, par exemple juridiques ou marketing, et se transformer en un risque systémique où un dysfonctionnement localisé produit des évènements en chaine, et peut alors entrainer des dommages dans toute la chaine de valeur.

…à la création de valeur pour l'entreprise

Le numérique au cœur de l'entreprise n'est créateur de valeur que s'il est stratégiquement implanté. Dans le cadre de la révolution numérique, vue comme une évolution majeure dans les modes de management et d'organisation de l'entreprise au XXIème siècle, l'entreprise numérique se différencie de l'entreprise traditionnelle par la volonté de tirer profit de la numérisation de son activité.

L'entreprise numérique n'est finalement pas qu'une *« entreprise tirant une part de sa valeur de la numérisation de ses activités, ses produits ou ses clients »* mais une entreprise qui *« tire sa valeur de la stratégie numérique qu'elle met en place »*.

« La gouvernance de l'entreprise se construit aujourd'hui avec une approche et ***une réflexion sur les risques.*** *C'est à la fois une exigence et un acte managérial. Il est vrai qu'au premier abord, l'entreprise numérique semble éviter des risques auxquels fait face l'entreprise classique. Mais ses caractéristiques propres génèrent de nouvelles sources de risques. »* [Extrait]

SOMMAIRE

INTRODUCTION

Cette étude vise à recenser tous les types de risques liés au caractère numérique d'une entreprise, ainsi que ceux qui sont susceptibles d'émerger lors de son passage vers le numérique. Cette liste des risques se veut exhaustive, mais ne doit pas faire perdre de vue l'importance relative de ces risques : alors que certains seront fréquemment rencontrés pour tout type d'entreprise, d'autres seront relativement ponctuels, voire exceptionnels.

Nous nous sommes limités dans ce rapport, aux risques ayant un lien direct avec l'activité numérique de l'entreprise. Partant de là, les menaces liées à la culture et aux usages numériques de la société, des consommateurs, des autorités… sont écartées. Par exemple, le fait qu'un *buzz* soit généré très rapidement et nuise à l'image de l'entreprise est un risque lié à la culture numérique de la société en général, et non pas au fait que l'entreprise soit numérique. Par ailleurs, nous avons focalisé notre attention sur les risques qui ont un lien réel (même indirect) avec le passage au numérique.

Enfin, ce rapport propose une cartographie et une représentation graphique des risques recensés. Il n'a pas pour objet de proposer des solutions concrètes sur la prévention et la gestion de ces risques, mais d'explorer *« ce qui pourrait arriver ».* Cette approche du sujet nous force à étudier la question du passage au numérique sous un angle négatif uniquement, laissant de côté cette composante intrinsèque de la notion de risque qu'est l'opportunité. En effet, à la lumière de la bibliographie et des entretiens réalisés, il apparait qu'au final, le plus grand risque serait justement de rater le passage au numérique. Il faut donc préciser que, si nous n'abordons ici que les éventuelles conséquences négatives de l'entreprise numérique, il faut garder à l'esprit les formidables opportunités qu'elle représente.

DÉMARCHE

L'analyse des risques liés au numérique nécessitait tout d'abord une réelle définition des termes de la problématique.
Si le concept de « risque » est celui qui parait le plus clair dans l'énoncé du sujet, sa définition n'en est pas pour autant figée et consensuelle. Étymologiquement, il viendrait de l'italien *risco*, mot dérivé du latin *resecum* (« ce qui coupe »), désignant le rocher qui menace les navires marchands[1] : autrement dit, le danger en mer. Ce concept est en lien avec le développement des assurances maritimes, notamment à Gênes, au XIVe siècle. Les deux premières définitions du risque données par le dictionnaire Larousse voient également le risque en termes de danger, et des dommages qui en résultent :
« 1. Possibilité, probabilité d'un fait, d'un évènement considéré comme un mal ou un dommage ; 2. Danger, inconvénient plus ou moins probable auquel on est exposé »

On voit donc qu'il y a 2 éléments essentiels dans la notion de risque : l'*évènement*, dont l'occurrence est probabilisable, qui va entraîner des conséquences négatives : un *dommage*, une perte. La géographie, discipline qui a longuement étudié les risques, a l'habitude de définir ceux-ci comme la confrontation d'un aléa (l'évènement possible) avec des enjeux (qui peuvent être endommagés)[2]. La seule présence d'un aléa ne suffit pas pour qu'il y ait un risque : que serait le virus sans la base de données importante qu'il doit détruire ? On peut le comparer à la crue d'un fleuve dans une zone non habitée : sans enjeux (vies humaines, maisons, industries…), l'aléa (crue) ne produit aucun dommage, il ne représente donc pas un risque.
La troisième définition proposée par le Larousse explique :
« 3. Fait de s'engager dans une action qui pourrait apporter un avantage, mais qui comporte l'éventualité d'un danger ».

Le risque est ici défini par deux composantes, une négative et une positive : le danger et l'opportunité. On se rapproche ici du « pari informatique »[3] évoqué par Bruno Ménard dans le cadre de la réflexion du CIGREF sur l'entreprise numérique. La numérisation est en effet une prise de risques, dans le sens où d'une part elle s'accompagne potentiellement d'évènements dangereux, et d'autre part, elle est une source d'avantages pour l'entreprise. Concernant le numérique, il semble que c'est bien cette troisième définition qui est la plus pertinente : le numérique est à la fois une formidable opportunité, et une source de nouveaux dangers dont il faut tenir compte.

[1] Patrick PERETTI-WATEL, *La société du risque*, Paris, La Découverte & Syros, collection Repères, 2001.
[2] Voir par exemple le site internet RISQUES MAJEURS : http://www.risquesmajeurs.fr/definition-generale-du-risque-majeur
[3] Voir sur le site Histoire Cigref : http://www.histoire-cigref.org/blog/le-pari-informatique/

Néanmoins, dans la mesure où cette étude concerne uniquement les risques liés au numérique, au sens ici de danger, nous écarterons cette définition, bien que nous soyons bien conscients de l'importance des aspects positifs de la numérisation. Nous optons donc pour la définition suivante, que nous avons construite à partir des différentes réflexions proposées ici :

Le risque est la conjonction d'un aléa (un évènement d'occurrence et d'intensité probabilisables ou non), et d'un enjeu (un élément qui a de la valeur, susceptible d'être endommagé par l'aléa).

Comment définir dans un deuxième temps l'entreprise numérique ? Existe-t-elle en l'état, est-ce une finalité, une entreprise étendue est-elle nécessairement numérique ? Aujourd'hui, toutes les entreprises communiquent par courrier électronique, utilisent des programmes de gestion et ont dématérialisé une partie de leurs activités (aussi infime soit-elle). Est-ce suffisant pour les qualifier de « numériques» ou seule une entreprise telle que Yahoo ou Google peut être considérée comme telle ?

Qu'englobe donc le concept d'entreprise numérique ? Une perspective qui aurait pu être intéressante mais qui, malheureusement, a vite montré ses limites est l'analyse du bilan de l'entreprise. En effet, cette vision financière de l'entreprise aurait pu mettre en évidence le profil de l'entreprise. Toutefois, trouver les éléments numérisés dans les comptes de l'entreprise est une mission assez délicate.

Après différentes propositions, issues des éléments de réflexion interne du CIGREF et de notre étude de la bibliographie, nous avons repris et synthétisé ces différentes idées au sein d'une définition simple :

Une entreprise numérique est une entreprise qui tire une part de sa valeur de la numérisation de ses activités, ses produits ou ses clients.

Une fois les principaux éléments définis, nous avons été confrontés au choix des outils d'analyse. En effet, quels outils utiliser pour aborder les risques associés au numérique pour les entreprises, pour pouvoir identifier leur impact sur celles-ci et identifier les sources de ces risques ?

Afin d'étudier toutes les dimensions inhérentes à la problématique, notre approche s'est appuyée sur deux axes principaux : interne et externe. Afin d'être le plus large possible, sans omettre aucun aspect, nous avons utilisé l'approche par parties prenantes (*stakeholders*) pour l'analyse externe et par « Chaîne de valeur » pour l'analyse interne.

La dimension *stakeholders* nous permet d'appréhender les différentes parties en interaction avec l'entreprise. Elle peut être définie comme « *tout individu ou groupe pouvant affecter ou être affecté par la réalisation des objectifs de l'organisation* » (Freeman, 1984). Concernant les risques numériques, il s'agissait de voir où pouvaient surgir ces risques, dans les relations

que l'entreprise entretient avec ses parties prenantes : les risques numériques liés aux consommateurs, aux actionnaires, aux fournisseurs, etc. Dans leur approche la plus large, les parties prenantes englobent :

- Dirigeants, salariés, syndicats
- Filiales
- Consommateurs en général
- Clients de l'entreprise
- Communauté locale
- Politiques, ONG, associations
- Régulateurs et gouvernements
- Sous-traitants, fournisseurs et cocontractants
- Institutions financières (assurances, banques)
- Concurrents
- Actionnaires.

Il faut bien noter qu'il n'existe pas nécessairement de risque numérique dans la relation qu'entretient l'entreprise avec chacune de ces parties prenantes. A l'inverse, il peut y avoir plusieurs risques vis-à-vis d'un seul de ces acteurs.

L'approche Chaîne de valeur nous permet d'être le plus exhaustif possible dans l'appréhension du fonctionnement de l'entreprise et cela de manière générique. La chaine de valeur est un modèle développé par M. Porter dans *L'avantage concurrentiel* (1986), qui vise à décomposer l'activité de l'entreprise en différentes étapes, pour identifier où se trouvent les sources d'avantages concurrentiels, autrement dit, de création de valeur. Malgré une conception de l'entreprise assez industrielle et peut-être un peu dépassée, sa richesse nous permet, grâce à quelques aménagements, de traiter tous les types d'entreprises.

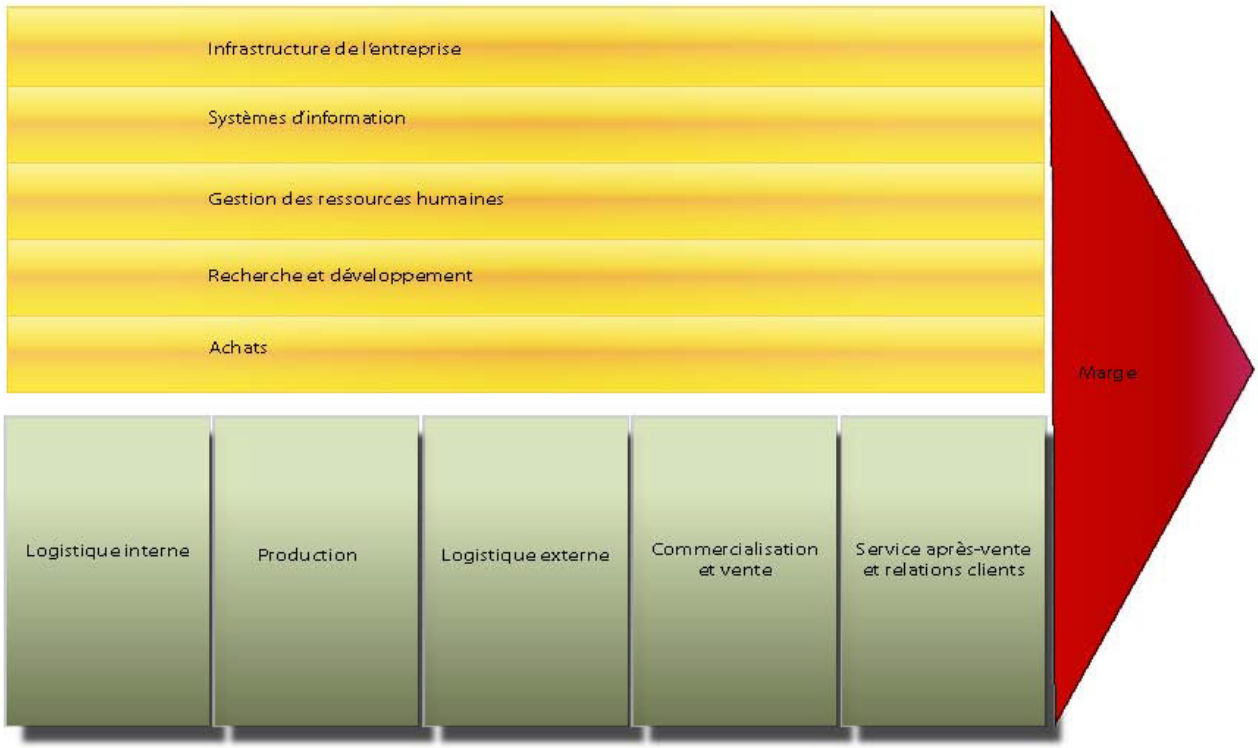

Figure 1 : Chaine de valeur de l'entreprise, modèle PORTER

Source : Kyomi ARRACHEA, Stéphane BOUCHE-OSOCHOWSKI, Youssef LAKHRI, novembre 2010

Ainsi, le croisement de ces deux approches permet une vue transversale et dynamique de l'entreprise en incorporant un maximum de variables d'analyse. Ces deux axes sont toutefois perméables. Certains risques peuvent donc être identifiés à la fois au niveau interne et externe.

Notre définition de l'entreprise numérique implique une mutation de la chaîne de valeur telle que Michael Porter la conçoit. En effet, selon sa conception, les systèmes d'information (SI) dans l'entreprise sont définis comme une fonction support. Toutefois, les mutations récentes au sein des entreprises plaident pour une vision radicalement différente. Les SI, et plus encore l'usage du numérique sous toutes ses formes, ne sont plus une fonction support à l'activité de l'entreprise mais deviennent une source même de la création de valeur au sein de celle-ci. C'est ainsi que nous concevons la définition de l'entreprise numérique. Le numérique intègre le cœur de la chaîne de valeur.

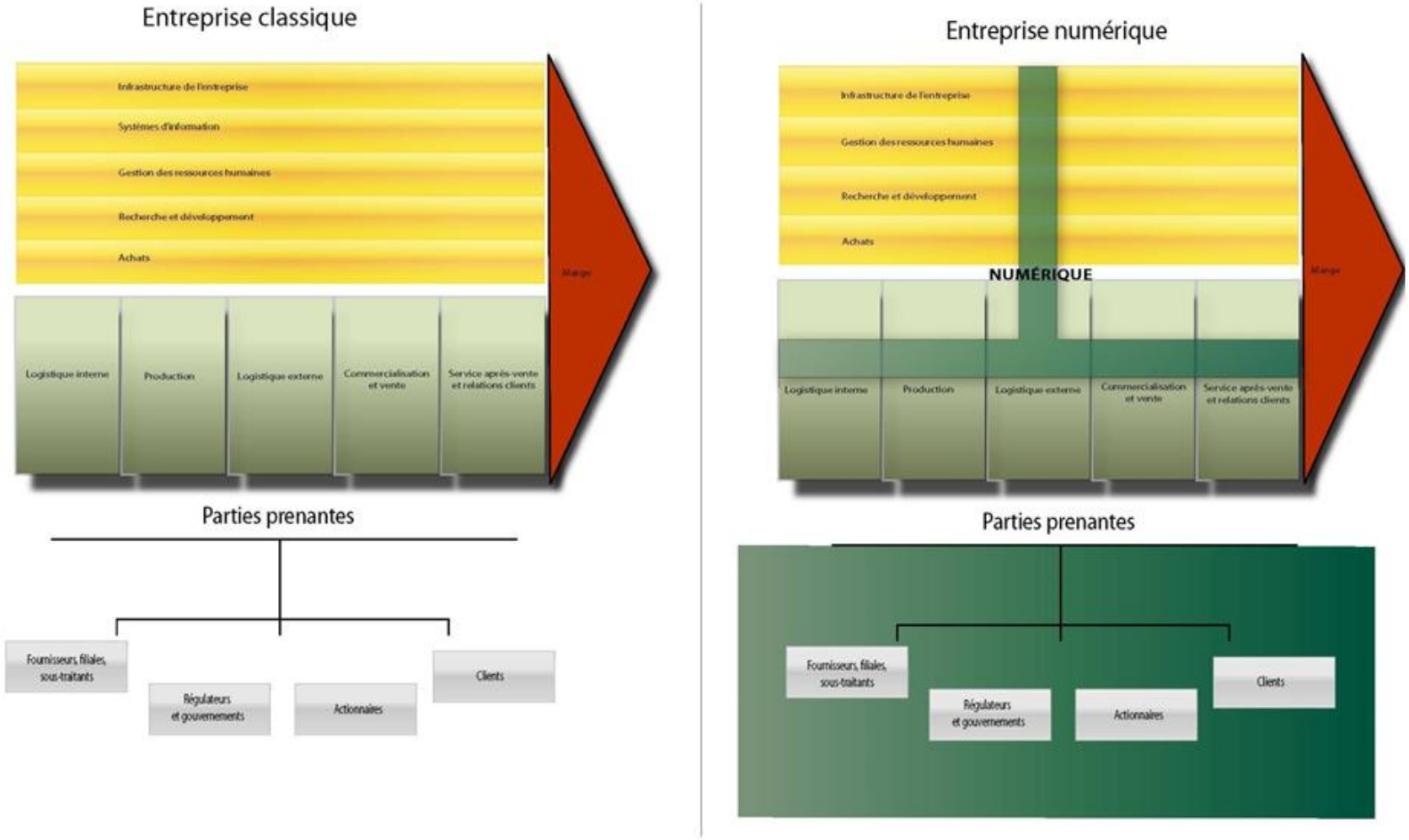

Figure 2 : Le passage à l'entreprise numérique

Source : Kyomi ARRACHEA, Stéphane BOUCHE-OSOCHOWSKI, Youssef LAKHRI, novembre 2010

LISTE DES RISQUES IDENTIFIÉS

Notre étude a mis en évidence huit branches de risques liés au numérique pour l'entreprise : des risques liés aux ressources humaines, des risques éthiques et juridiques, des risques liés au contrôle et à la maîtrise du système d'information, mais aussi des risques liés à la stratégie de numérisation de l'entreprise, au marketing, au patrimoine, ou plus généralement à la dématérialisation des rapports humains. Une dernière catégorie se détache enfin, celle des risques périphériques à l'entreprise.

1. RISQUES LIÉS AUX RESSOURCES HUMAINES

La gestion des ressources humaines peut être fortement impactée lors de la numérisation de l'entreprise, du fait de la rupture des usages liée au numérique notamment. En effet, l'arrivée du numérique dans une entreprise s'accompagne parfois de licenciements, de changements dans les habitudes quotidiennes de travail ou nécessite de nouvelles formations… Or, ces changements affectent directement le facteur humain de l'entreprise, et sa réaction négative potentielle impacte le résultat de l'entreprise par une diminution de sa productivité ou un ralentissement de son activité. Nous identifions donc trois risques majeurs attachés aux ressources humaines : le manque d'adhésion ou le rejet par les employés de la politique de numérisation de l'entreprise, les risques sociaux et enfin la sclérose des compétences.

Le manque d'adhésion ou le rejet de la politique de numérisation de l'entreprise par les employés. Sans mettre en place des pratiques de management dans le cadre de la conduite du changement, l'entreprise peut se retrouver face à une attitude hostile de ses salariés lors de la numérisation des activités de l'entreprise. Cette hostilité s'exprime de différentes manières, d'un simple malaise jusqu'au rejet du nouvel outil numérique. Ici, la numérisation de l'entreprise aura eu lieu, mais engendrera des pertes au lieu de créer de la valeur.

La sclérose des compétences. Rappelons avant tout que le domaine des NTIC connait une évolution extrêmement rapide. Une innovation technologique peut ainsi rendre obsolète les compétences des employés dans certains secteurs spécifiques, cela est d'autant plus vrai dans certains secteurs tels que l'utilisation des progiciels par exemple. Les TIC connaissent une évolution tellement rapide qu'il devient parfois plus intéressant pour une entreprise d'embaucher de jeunes diplômés formés à la dernière technologie plutôt que de former ses anciens employés.

Les risques sociaux. Enfin, l'hostilité des salariés vis-à-vis de la numérisation de l'entreprise doit être considérée différemment si elle prend une forme collective organisée. Dans les cas précédents, nous étions face à des comportements isolés. Il est également possible de se trouver face à une contestation organisée, surtout si la rupture entrainée par la numérisation a entrainé des licenciements. Le risque est alors de voir la productivité diminuer, voire s'immobiliser en cas de grève. Ce risque peut également se reverser sur d'autres pans de l'entreprise et alimenter d'autres sources de crises pour celle-ci.

2. RISQUES ÉTHIQUES ET JURIDIQUES

Les risques éthiques et juridiques liés au numérique dans l'entreprise renvoient à la fois au respect de la vie privée et la confidentialité des données mais aussi à l'inégale vitesse d'évolution des technologies et des usages associés (actuellement très rapides) avec le droit. Les activités permises par l'internationalisation des entreprises (stockage des données à l'étranger, etc.) et les problèmes liés à l'authenticité des documents numériques font également partie des risques juridiques auxquels doit faire face l'entreprise numérique.

Respect de la vie privée et confidentialité des données. Lorsqu'une entreprise décide de numériser des données personnelles (relatives à des clients ou des collaborateurs…), elle a l'obligation de déclarer ces données à la CNIL, ainsi que d'en assurer la sécurité (contrairement à des données non numériques). L'entreprise fait donc face à des risques juridiques liés à cette obligation légale de sécurisation de ces données.

Évolution du droit. Le droit français concernant le numérique date de 2000. Cependant, dans la mesure où la technologie et les usages évoluent très rapidement, il est logique que le droit doive évoluer aussi pour répondre aux nouvelles questions générées par ces changements. Les conséquences pour l'entreprise peuvent être des pertes liées à la mise en conformité avec de nouvelles lois. Ou inversement, le droit peut évoluer beaucoup moins rapidement et donc créer des situations sans aucune possibilité, en cas de besoin, de se référer à la loi afin que l'entreprise puisse se défendre ou attaquer en justice.

Contexte d'application des décisions de justice. Certaines questions concernant le numérique (par exemple, la gestion des contentieux commerciaux) laissent une part d'appréciation importante au contexte judiciaire. Par ailleurs, la jurisprudence n'est pas encore très développée. L'entreprise peut donc se retrouver confrontée à l'incertitude liée aux différences de contexte d'application des décisions de justice, ce qui peut entraîner des pertes.

Internationalisation. Des informations sur l'entreprise peuvent circuler à l'étranger via le jeu des réglementations internationales ou être soumises à des réglementations locales. Par exemple, les serveurs de données situés aux États-Unis sont soumis au *Patriot Act*, et la NSA a donc le droit de consulter les données qu'ils contiennent, ce qui présente un risque pour l'entreprise qui possède de tels serveurs (ou qui sous-traite l'hébergement de ses données à un fournisseur dont les serveurs sont situés sur le sol américain). Plus généralement, la législation concernant l'échange de données est différente selon les pays, le cryptage peut être autorisé, interdit, soumis à autorisation… Pour l'entreprise, cela se traduit concrètement par des pertes en cas de non respect de la loi locale, ou des problèmes de productivité et d'homogénéisation des processus dans le cadre d'une activité internationale.

Authenticité des documents. L'authenticité des documents numériques est plus difficile à prouver que celle des documents papier ; leur production et leur conservation entrainent donc plus de contraintes (et de risques). Ces contraintes sont essentiellement liées à l'administration, par exemple pour les documents comptables qui doivent répondre à certaines normes techniques (présentation de la pièce justificative). Si ces données sont

hébergées dans un autre pays, réparties sur différents sites (qui ne respectent peut-être pas les normes), ou non accessibles pendant un moment… en cas de contrôle fiscal, l'entreprise fait face à un risque juridique.

3. RISQUES LIÉS AU CONTRÔLE ET À LA MAITRISE DU SI

L'un des principaux gains entrainés par la numérisation de l'entreprise est un gain de temps. La numérisation fluidifie l'information et lui permet de circuler plus vite, ce qui a pour effet de créer de la valeur. Mais, par définition, plus l'information est fluide, plus elle est rapide, et moins on en a le contrôle. La question pour l'entreprise sera de savoir où elle souhaite se situer entre l'absence de contrôle et le contrôle total de l'information (ce qui aurait pour effet de faire perdre tout gain à la numérisation de celle-ci). Plus le contrôle est grand, plus l'exposition à un ralentissement de l'activité de l'entreprise est importante. Moins le contrôle est important, plus l'exposition à des fuites d'informations est grande. Le risque pour l'entreprise est de voir alors ses données dérobées, altérées ou modifiées. Ce dommage peut résulter de plusieurs facteurs.

Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des employés. Nous sommes ici dans le cadre d'une malveillance interne. L'employé qui a accès au réseau interne de l'entreprise peut potentiellement l'utiliser pour lui faire du mal. La gravité dépend de l'information à laquelle il accède. Ce risque n'est pas à négliger et les employés ont généralement une bonne connaissance des failles de sécurité de l'entreprise.

Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des pirates. Il ressort de notre étude que les attaques essuyées par l'entreprise du fait de hackers étaient assez rares. Le pirate doit en effet avoir une raison particulière pour s'attaquer à l'entreprise. Si le phénomène « hacker » est très médiatisé, il n'en reste pas moins que les auteurs des actions les plus dommageables restent les employés de l'entreprise.

Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des programmes malveillants (virus). Ce genre de dommage peut également être causé par tout type de programme malveillant. Si la menace est quotidienne, le dommage n'est généralement pas très important. La réponse à apporter est généralement assez simple.

La négligence des salariés. Au-delà des risques dus à la malveillance, on retrouve également des risques liés au comportement négligent des employés. Ce comportement est produit le plus souvent par une méconnaissance des enjeux de sécurité de l'entreprise pour le salarié ou par des usages de travail (partage des sessions, des mots de passe, etc.). Cette négligence peut entraîner vol/altération/modification des données de l'entreprise.

Déni de service entrainé par la saturation de réseaux ou des processus. Utiliser le numérique entraine une utilisation croissante du réseau de l'entreprise, une sollicitation plus importante des processus numériques mis en place et cela peut entraîner une saturation. Cette saturation se traduit par un ralentissement (parfois une immobilisation) tel que l'entreprise n'est plus en mesure de produire, de communiquer ou de fournir son client. Ce

risque de déni de service peut avoir une source interne (ex : saturation du logiciel de facturation) ou une source externe (ex : problème technique chez le sous-traitant en *Cloud computing*).

Ralentissement des activités de l'entreprise du à la rigidité des procédures de contrôle liées à la numérisation (type droits d'accès). Le dernier risque identifié est un risque lié à la gestion même du risque. Si l'entreprise numérique choisit de contrôler son information au maximum, elle peut ralentir très significativement son activité et induire une diminution de la création de valeur, souvent synonyme de perte. Les *workflow* peuvent créer de réels ralentissements d'activité.

4. RISQUES STRATÉGIQUES

D'autres risques liés au numérique se détachent du quotidien de l'entreprise et sont liés aux processus de décision engagés sur le moyen et le long terme. Le passage de l'entreprise classique à l'entreprise numérique suppose de prédéfinir un plan stratégique de la numérisation des activités de l'entreprise, et ce en accord avec l'objectif final : voir naître de la valeur de cette numérisation et surtout de son utilisation.

La défaillance de stratégie numérique. Le plus grand risque lié à la stratégie de l'entreprise est bien d'avoir une stratégie numérique défaillante, ou pire encore, de ne pas avoir de stratégie numérique du tout. Le passage au numérique pour l'entreprise peut être motivé par de multiples facteurs, et les décisions être parfois mal pesées, notamment par manque de culture numérique. Une déficience stratégique entraine des conflits internes à l'entreprise (concurrence entre fonction numérique et fonction non numérique) ou des pertes suite à la numérisation d'activités de l'entreprise qui n'auraient pas du l'être. Un des risques majeurs identifiés par certains DSI est la disparition même de la Direction des SI de l'entreprise. Les solutions externes sont déjà prêtes à l'emploi, alors que développer les systèmes en interne demande beaucoup plus de temps.

Le *lock in*. Il s'agit de la situation dans laquelle une entreprise est dépendante d'un fournisseur et ne peut passer à la concurrence que pour un coût prohibitif. Le *lock in* est particulièrement présent dans le monde de l'informatique, aussi les décisions stratégiques des fournisseurs peuvent avoir de lourdes conséquences, notamment dans le cadre du *cloud computing*. Être enfermé peut empêcher l'interopérabilité des systèmes en interne et en externe, mais aussi entrainer une incapacité à évoluer qui entraine une perte de l'avantage concurrentiel, finalement un manque à gagner voire une perte.

La concurrence entre deux supports de vente. Nous sommes dans le cas où la numérisation de l'entreprise porte sur sa capacité de vente, par exemple en ouvrant un site internet de vente en ligne. Le manque de planification dans la stratégie numérique ou la réaction du marché (engouement pour la plateforme *online*) entraine la cannibalisation : au lieu de gagner des clients, l'entreprise va voir ses deux points de vente se partager les mêmes, et dans certains cas voir la disparition du point de vente.

5. RISQUES MARKETING

Les risques induits par la numérisation de l'entreprise et liés au secteur marketing sont de différente nature et affectent la réputation de l'entreprise ou bien sa capacité de vendre à des clients.

Risque réputation. Un site internet est un outil vulnérable. C'est un outil de communication et de marketing de premier plan qui peut être la cible de personnes malveillantes à l'égard de l'entreprise. Ceci est d'autant plus facile lorsque le site propose une plateforme de communication *bottom-up*. Que ce soit une campagne organisée ou de réels mécontentements, l'entreprise court un risque réel en termes d'image en offrant un espace de liberté au cœur de son outil de communication.

Augmentation de la concurrence. La numérisation de l'entreprise peut tout simplement porter sur sa capacité à vendre en ligne. Mais comme pour un point de vente physique, elle va trouver sur ce marché internet des concurrents. Or, ces concurrents ne sont pas uniquement de la même ville ou du même pays, ils sont installés dans le monde entier. La dématérialisation des clients et des points de vente fait entrer sur un marché potentiellement mondial, mais sur lequel la concurrence est bien plus forte. De plus le développement des comparateurs de prix de plus en plus diversifiés implique une concurrence accrue pour l'entreprise. Cela est d'autant plus vrai pour les produits « standardisés ».

6. RISQUES LIÉS À LA DÉMATÉRIALISATION DES RAPPORTS HUMAINS

Le passage vers l'entreprise numérique implique également la dématérialisation – et non la disparition – des rapports humains. Cette dématérialisation se retrouve dans les relations entre collègues mais aussi avec l'extérieur, clients et fournisseurs.

Affaiblissement de la communication. La mutation des rapports sociaux entraine également une mutation de la communication. Bien que nous ayons des moyens plus performants et plus nombreux pour communiquer, la tendance à moins communiquer existe potentiellement, la qualité de cette communication peut également diminuer et c'est ce dernier point qui est important à prendre en compte pour l'entreprise. Cela est appelé le Paradoxe de Maslow. L'instant machine à café et discussions directes est moins développé (notamment à cause du télétravail) ce qui implique moins d'interactions entre les employés.

Perte de souplesse. La numérisation des process de l'entreprise simplifie souvent les procédures de décision, notamment dans le secteur de la banque. Mais cela se fait au détriment de phases de discussion et d'échange (avec le client, le fournisseur ou le salarié). Si cela fait gagner du temps, l'entreprise peut perdre en souplesse et en adaptabilité et ainsi risquer de devenir trop rigide par rapport à la concurrence.

Perte du temps de réflexion. L'accélération de l'économie et des échanges dus à la numérisation de l'information laisse moins de temps à l'acteur économique (client,

fournisseur, entreprise, employé, dirigeant) pour penser. Le risque pour l'entreprise est de se retrouver dans une situation où elle n'a plus la capacité à anticiper. Elle se place dans la réactivité, au détriment d'une réflexion en amont.

Infobésité. L'infobésité fait référence à la surabondance d'information numérique présente quotidiennement et sous toutes ses formes. Une bonne communication nécessite l'utilisation de plusieurs canaux. Or, la dématérialisation des rapports humains entraine une augmentation nette du volume d'information numérique traitée par les employés de l'entreprise. Celle-ci risque donc de voir ses canaux de communication saturés et une part de l'information sera perdue ou mal traitée.

7. RISQUES LIÉS AU PATRIMOINE NUMÉRIQUE

Dans cette famille de risques, nous avons englobé les risques liés à la conservation numérique des données (vieillissement des supports, évolution des formats), à la difficile valorisation financière du patrimoine numérique ainsi que ceux liés à la garantie des produits numériques.

Conservation. On a vu précédemment que la conservation de données numériques exposait l'entreprise à des risques juridiques. Une mauvaise conservation de telles données peut aussi entraîner des pertes pour l'entreprise : la durabilité des supports et des formats n'est pas facile à assurer dans le cadre du stockage numérique. Par ailleurs, les entreprises sous-traitent souvent cet hébergement des données numériques, donc le contrôle sur les mesures de protection et conservation ne peut être facilement assuré, de même que l'accès à ces données peut être temporairement coupé. Enfin, il ne faut pas exclure les risques liés aux catastrophes naturelles, qui peuvent affecter les *datacenters*, et donc impacter gravement les entreprises numériques en paralysant ou ralentissant leur activité.

Valorisation financière. Les méthodes pour calculer la valeur d'une entreprise sont mal adaptées au calcul de la valeur d'une entreprise 100% numérique. En effet, celle-ci ne dispose pas d'actifs réels mais immatériels, dont la valorisation est difficile. La valeur de l'entreprise numérique peut donc être mal évaluée par les institutions financières, ce qui a des conséquences au niveau de ses actionnaires et investisseurs. Par ailleurs, la sous-évaluation de l'entreprise numérique peut entraîner des difficultés vis-à-vis des institutions bancaires, qui peuvent refuser de la financer, ce qui peut provoquer un risque important pour la poursuite des activités ou le développement de l'entreprise.

Produits non garantis. Les risques liés au patrimoine numérique englobent également les risques liés à la garantie des produits numériques ; celle-ci n'étant pas toujours aussi clairement définie que pour des produits matériels ce qui entraîne un nouveau risque pour les entreprises. Les conséquences des problèmes rencontrés lors de l'utilisation de tels produits sont ainsi à assumer par les entreprises qui les utilisent, qui ne peuvent pas se retourner contre les fabricants. L'entreprise assume donc le risque lié à l'utilisation des produits numériques.

8. RISQUES PÉRIPHÉRIQUES

Cette dernière famille de risques regroupe le risque lié à la perte de contrôle du produit et le risque géopolitique, qui, s'ils apparaissent comme exceptionnels, n'en sont pas moins potentiellement dangereux pour l'entreprise.

Perte de contrôle du produit. Depuis le début des années 80 et l'avènement de l'informatique, et plus récemment du numérique, il s'avère qu'une partie de l'économie s'est largement dématérialisée. Les flux d'informations et les flux financiers ont connu une croissance exponentielle en moins d'une quinzaine d'années. La dématérialisation des flux a montré par le passé que les risques et leurs impacts ont été démultipliés. Grace à la numérisation, tout se trouve amplifié, accéléré et de ce fait devient moins contrôlable. C'est ainsi que nous avons vu se développer la crise des pays asiatiques, la quasi faillite de l'Angleterre (due à la spéculation du fond d'investissement de Soros), la crise des *subprimes* (les banques ne sachant plus dans un premier temps si elles possédaient ou non des *Crédit Default Swap*). Tous ces événements sont symptomatiques des risques périphériques à l'entreprise (et parfois à l'État) dont les impacts sociaux et économiques ne sont peut être pas identifiables en amont mais dont les conséquences peuvent être dévastatrices. La numérisation de l'entreprise implique une refonte des pratiques de bonne gouvernance.

Risque géopolitique. On pourrait croire au premier abord que l'entreprise numérique s'affranchit en grande partie du risque pays, mais en réalité celui-ci continue à exister, sous d'autres formes, avec le numérique. On peut citer l'exemple du Myanmar, où des attaques de DDoS (attaques par déni de service -*denial of service* attack) ont isolé le pays du réseau internet pendant les sept jours précédant les premières élections politiques en 20 ans (et où l'origine politique de cet acte peut être suspectée). A une toute autre échelle, les guerres, et le recours à des IEM (impulsions électromagnétiques, ou EMP en anglais), peut entièrement paralyser l'entreprise numérique.

CARTOGRAPHIE DES RISQUES

La cartographie des risques a été réalisée selon les étapes suivantes : un recensement des risques, leur classement graphique en fonction de l'occurrence et de la gravité, et enfin la schématisation de leur représentation.

Tout d'abord, nous avons qualifié chacun de ces risques par un degré d'occurrence et un degré de gravité, qui vont chacun de 1 à 10 (1 étant le plus faible, 10 étant le plus élevé).

Ensuite, un facteur de risque a été élaboré, en multipliant le degré d'occurrence et le degré de gravité, aboutissant ainsi à un indice situé entre 1 (facteur de risque faible) et 100 (facteur de risque élevé). Il s'agit là d'une méthodologie couramment utilisée en cartographie des risques[4]. Les indices de gravité et d'occurrence ont été attribués à partir de notre analyse, basée sur les entretiens auprès de professionnels et la bibliographie que nous avons étudiée. Pour approfondir cette analyse, une piste de recherche consisterait à soumettre ces indices lors d'une enquête auprès de différents acteurs et notamment les DSI.

RECENSEMENT DES RISQUES

Famille de risques	Risques	Identifiant	Facteur de risque
Risques RH	Manque d'adhésion/rejet des employés à la politique de numérisation	RH1	40
	Sclérose du personnel	RH2	20
	Ralentissement de l'activité de l'entreprise du aux risques sociaux	RH3	18
Risques éthiques et juridiques	Risque de perte de confidentialité	EJ1	25
	Respect de la vie privée	EJ2	16
	Évolution du droit	EJ3	16
	Imprévisibilité de la justice	EJ4	12
	Internationalisation	EJ5	36
	Perte de la valeur authentique des documents	EJ6	25
Risques liés au contrôle et à la maitrise du SI	Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des employés	SI1	15
	Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des pirates	SI2	14

[4] Gilbert DE MARESCHAL, *La cartographie des risques*, Saint-Denis : AFNOR, collection À savoir, 2003, 50 p.

Famille de risques	Risques	Identifiant	Facteur de risque
	Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des programmes malveillants (virus)	SI3	21
	Vol/altération/modification de données de l'entreprise suite à la négligence d'un employé	SI4	12
	Déni de service entraîné par la saturation de réseaux (interne)	SI5	15
	Déni de service entraîné par la saturation de réseaux (externe)	SI6	12
	Ralentissement de l'activité de l'entreprise due aux procédures de contrôle	SI7	18
Risques stratégiques	Conflits internes dus à un défaut de stratégie numérique	ST1	28
	Perte entraînée par la numérisation d'aspects qui n'auraient pas du l'être (numériser pour numériser)	ST2	24
	Lock in	ST3	18
	Concurrence entre des supports de vente	ST4	21
Risques marketing	Réputation	MK1	20
	Augmentation de la concurrence	MK2	24
Risques liés à la dématérialisation des rapports humains	Diminution de la quantité et de la qualité de la communication	DM1	28
	Perte de souplesse	DM2	32
	Réaction plus que réflexion	DM3	21
	Infobésité	DM4	24
Risques liés au patrimoine	Conservation (y compris catastrophes naturelles)	PA1	28
	Valorisation financière	PA2	30
	Produits non garantis	PA3	12
Risques périphériques	Risques dus à la perte de contrôle du produit (cf. titrisation)	PE1	16
	Risques pays (guerre, DDoS, EMP)	PE2	9

Source : Kyomi ARRACHEA, Stéphane BOUCHE-OSOCHOWSKI, Youssef LAKHRI, novembre 2010

CLASSEMENT GRAPHIQUE DES RISQUES

Une première cartographie consiste à placer sur un graphique chacun des risques, selon leur indice d'occurrence (en abscisse) et leur indice de gravité (en ordonnée).

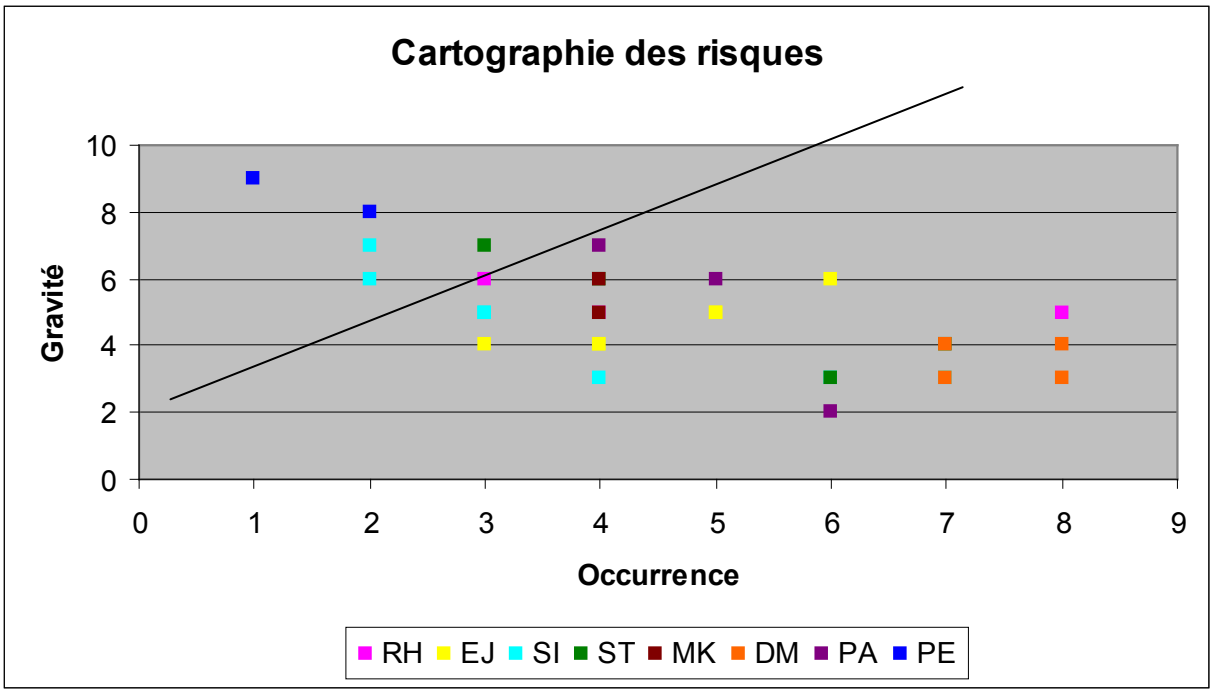

Figure 3: Cartographie des risques

Source : Kyomi ARRACHEA, Stéphane BOUCHE-OSOCHOWSKI, Youssef LAKHRI, novembre 2010

La lecture de ce graphique, au premier abord, ne fait pas apparaître des regroupements très clairs. On observe bien que, comme dans tout autre type de risques, leur occurrence est inversement proportionnelle à leur gravité (dans leur allure générale). La droite tracée sur le graphique représente une frontière qui délimite les risques dont il faut se soucier à court terme (forte occurrence, et faible gravité), des risques dont il faut se préoccuper à moyen/long terme (plus faible occurrence, et forte gravité).

A partir de ce graphique, on peut effectuer une première typologie des risques, pour essayer de dégager des tendances : on peut regrouper ainsi des risques proches, en termes de gravité et d'occurrence.

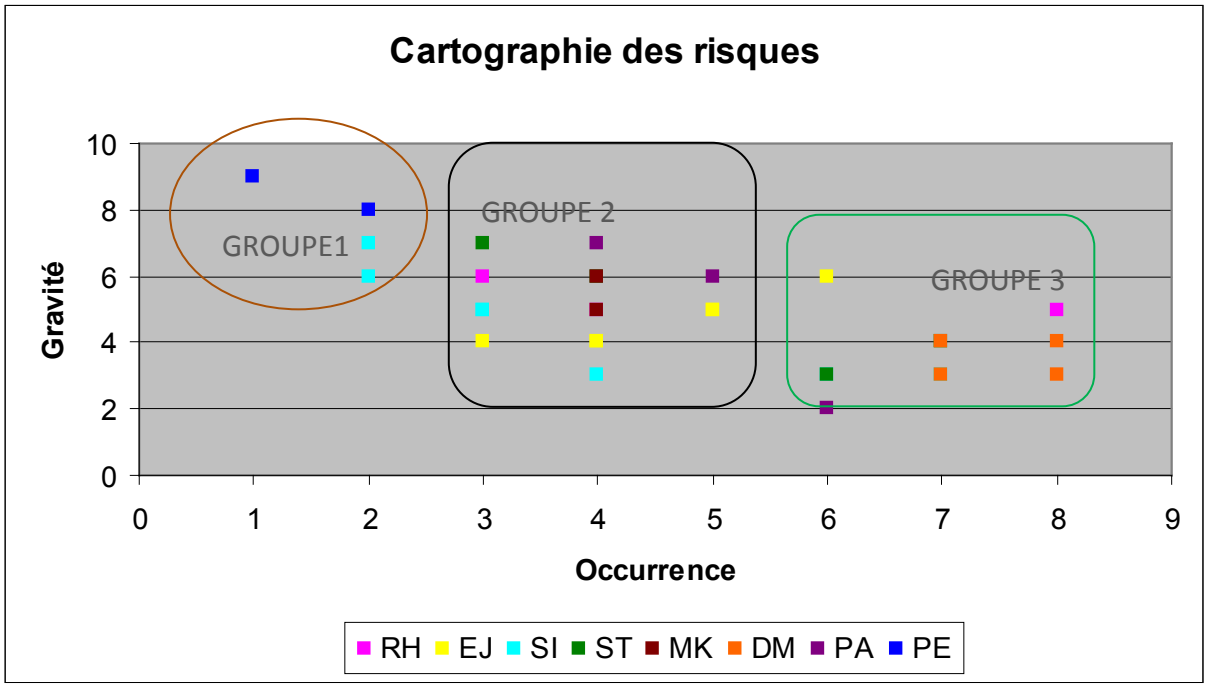

Figure 4: Cartographie des risques

Source : Kyomi ARRACHEA, Stéphane BOUCHE-OSOCHOWSKI, Youssef LAKHRI, novembre 2010

Le groupe 1 représente les risques à faible occurrence et à forte gravité, ceux que l'on appelle communément « risques majeurs ». On y retrouve les deux risques périphériques, ainsi que deux risques liés à la maitrise du système d'information : le risque lié à l'altération de données par des pirates, et le risque de déni de service (externe). Il s'agit là de phénomènes très peu fréquents, mais qui peuvent avoir de lourdes conséquences pour l'entreprise. Souvent, les risques majeurs sont peu pris en compte dans la mesure où leur occurrence est extrêmement faible : c'est probablement le cas des deux risques périphériques cités ici, néanmoins, il semblerait que les risques liés aux systèmes d'information soient au cœur des préoccupations des divers acteurs de l'entreprise, ou du moins très présents dans les esprits. Dans tous les cas, leur prévention est d'autant plus difficile que l'on ne peut guère savoir les modalités de leur occurrence (celle-ci étant très faible), et que leurs conséquences sont de grande ampleur.

Le groupe 3 rassemble les risques très fréquents, mais de relative gravité. Il est possible d'observer que la totalité des risques liés à la dématérialisation des rapports humains s'y trouve : on peut ainsi en déduire qu'il est très difficile de dématérialiser une activité sans prendre le risque de diminuer la qualité, la quantité, la souplesse dans la communication, ou de se retrouver noyé dans la surenchère d'information, à laquelle il faut réagir rapidement. De même, on comprend que les risques RH liés à la conduite du changement appartiennent à cette catégorie. A partir du moment où l'on sait qu'ils sont quasiment inhérents aux procédures de numérisation, ces risques peuvent facilement être pris en considération et gérés à l'avance : la prévention en est d'autant plus facilitée.

Enfin, le groupe 2 réunit le reste des risques, à occurrence et à gravité moyennes, qui se distinguent moins du lot par leur gravité ou leur probabilité de survenance. Le défi pour l'entreprise est alors de les identifier (tous n'accompagnent pas nécessairement chaque projet de numérisation), et de les gérer proportionnellement à leur facteur de risque.

Un deuxième type de cartographie consiste en la représentation, sous forme d'histogramme, du facteur de risque. Nous avons classé les risques du plus important au plus faible.

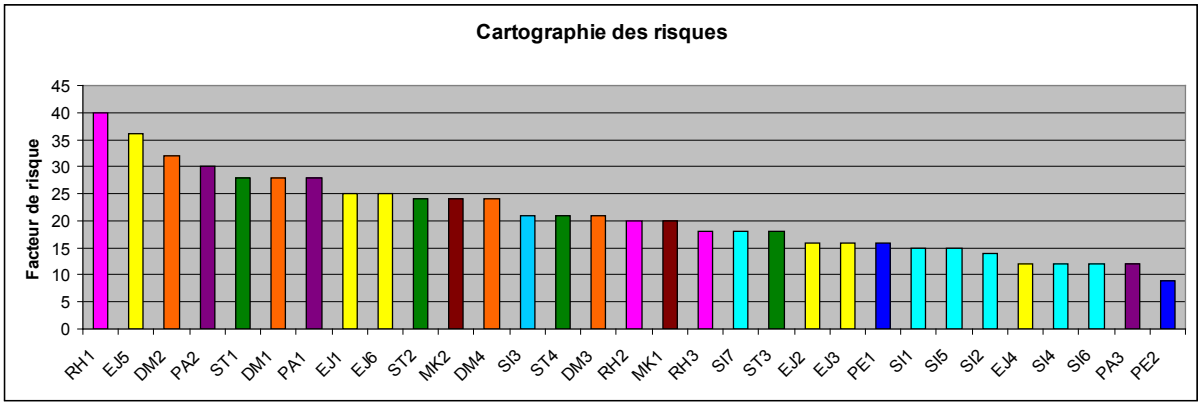

Figure 5: Cartographie des risques

Source : Kyomi ARRACHEA, Stéphane BOUCHE-OSOCHOWSKI, Youssef LAKHRI, novembre 2010

Ce graphique met en valeur d'autres problématiques que le précédent. En effet, il apparaît que le risque le plus important est RH1, soit le manque d'adhésion ou le rejet des employés vis-à-vis de la politique de numérisation, alors qu'il apparaissait, dans le graphique précédent, dans le groupe 3 (occurrence importante, gravité relative), et qu'il ne se distinguait pas particulièrement. En réalité, il s'agit d'un phénomène très couramment rencontré (8), dont la gravité est moyenne (5), ce qui aboutit à un facteur de risque de 40, soit le plus important. Tous les entretiens ont fait ressortir ce risque, l'importance que les acteurs lui donnent est assez forte, ce qui confirme bien sa première place dans le classement.

Le deuxième risque le plus important, EJ5, soit les risques juridiques liés à l'internationalisation des activités, ne se distinguait pas non plus dans le graphique précédent. Sa probabilité d'occurrence comme sa gravité sont moyennes (6), mais il ne concerne pas nécessairement avec la même importance toutes les entreprises qui choisissent de se numériser, car toutes ne rencontrent pas nécessairement des problématiques internationales.

Parmi les risques les plus faibles, on retrouve bien évidemment les risques périphériques (car leur occurrence est très limitée, même si leur gravité est très forte), et la plupart des risques liés à la maîtrise des SI : en effet, ceux-ci, bien que très présents dans l'imaginaire culturel et faisant l'objet de nombreux débats et mesures de prévention, ne sont finalement

pas très élevés. Ces risques sont finalement bien connus, bien identifiés, et leur fréquence ou leurs conséquences ne sont pas particulièrement importantes.

Ceci nous permet finalement de cartographier les risques sur la chaine de valeur de l'entreprise numérique (voir page suivante).

CARTOGRAPHIE SUR CHAÎNE DE VALEUR DE PORTER (CCVP)

La CCVP permet de situer les risques aux différents stades de l'organisation de l'entreprise et de comprendre leur importance dans le processus de création de valeur. Cet outil permet au dirigeant ou au DSI en charge de la question d'adapter ses réponses de manière précise et ajustée. Les risques mis en évidence présentent ainsi deux caractéristiques selon qu'ils soient localisés ou omniprésents, internes ou jouant sur les relations avec les parties prenantes.

Les risques localisés se retrouvent à des endroits précis de la CCVP. Il en est ainsi des risques marketing par exemple que nous voyons apparaître en fin de chaine de valeur. Le dirigeant trouvera donc des réponses à ces risques au niveau des départements commercialisation / vente et SAV de l'entreprise.

D'autre part, des risques trouvent leur origine dans l'interaction avec les parties prenantes, c'est le cas des risques éthiques et juridiques, souvent liés aux réglementations des États et aux accords de branche.

Enfin, les risques omniprésents présentent des défis stratégiques plus complexes dans la mesure où ils impactent l'entreprise à tous ses niveaux. C'est le cas des risques RH ou plus encore des risques stratégiques qui sont transversaux dans la CCVP. Ils influent directement sur toute la chaine de valeur. Aussi, une mauvaise décision stratégique joue sur tout le processus de production de l'entreprise et affecte la marge en bout de chaine. En combinaison avec la lecture statistique, ces risques apparaissent ainsi primordiaux dans le développement numérique de l'entreprise.

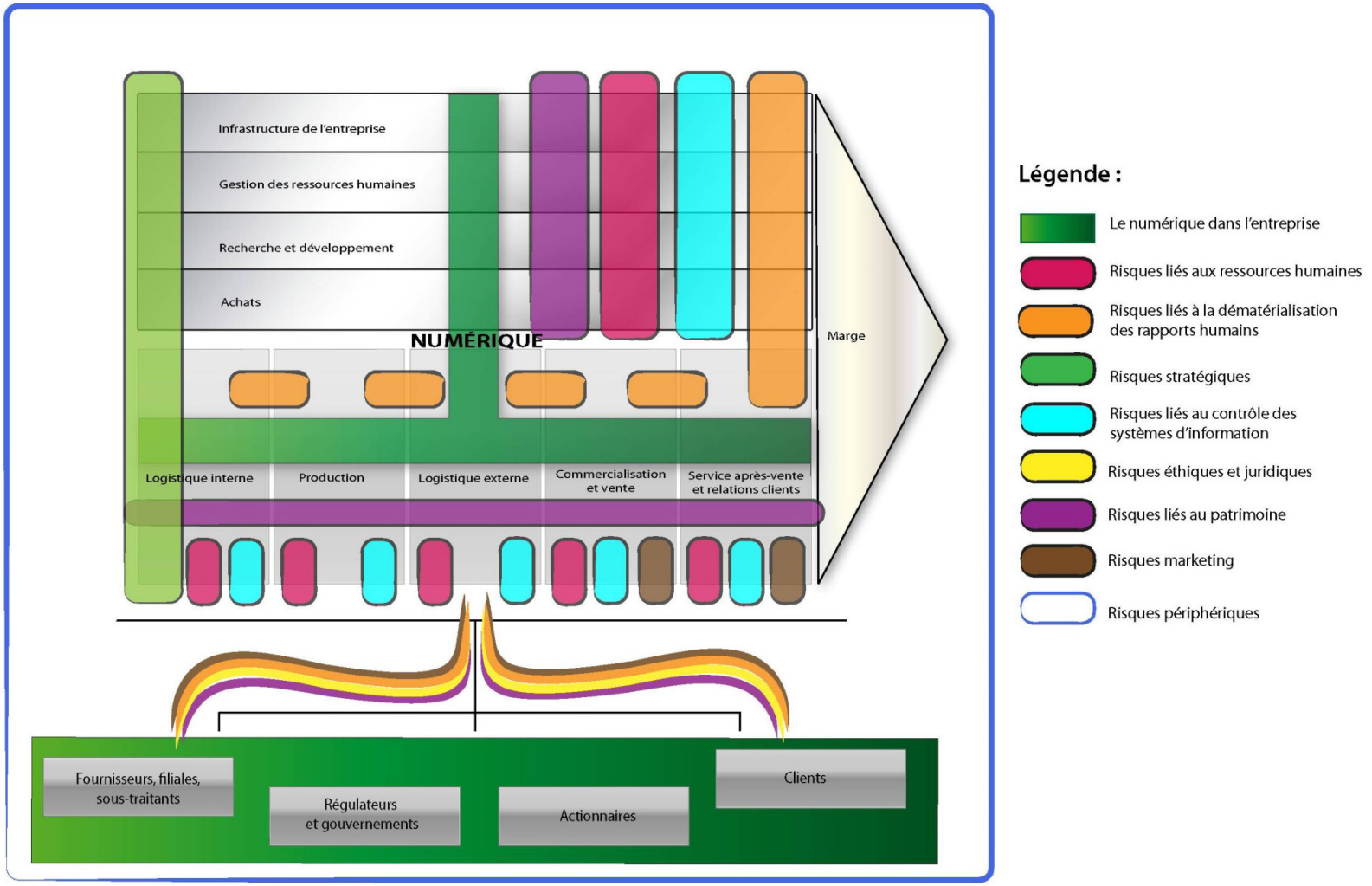

Figure 6: Cartographie des risques numériques pour l'entreprise

Source : Kyomi ARRACHEA, Stéphane BOUCHE-OSOCHOWSKI, Youssef LAKHRI, novembre 2010

CONCLUSION

Après cette étude, nous pouvons tirer quelques conclusions générales qui permettent de mieux comprendre les risques liés au numérique et à leurs interactions. Tout d'abord, nous avons vu qu'il existe un nombre important de risques, dont les conséquences s'appliquent à des domaines très différents dans l'entreprise : les métiers, les relations avec les parties prenantes…

Comme nous l'avions postulé au départ, les risques liés au numérique ne sont pas circonscrits au seul périmètre des systèmes d'information, mais sont transversaux, dans la mesure où le numérique est au cœur de la chaîne de valeur de l'entreprise. Cela ne veut pas pour autant dire que *« tout est dans tout »* : ainsi, certains risques sont plus localisés, comme les risques marketing (concentrés sur la fin de la chaîne de valeur et les relations avec les clients). On notera également que tous les risques n'apparaissent pas au même moment : alors que certains seront d'actualité tout au long de la vie de l'entreprise (comme ceux relatifs à la cybercriminalité), d'autres n'apparaissent qu'au moment du passage vers le numérique, pour s'estomper ensuite (par exemple le risque lié au manque d'adhésion des employés, ou celui lié à la concurrence entre supports de vente). Ces distinctions sont importantes lorsqu'il s'agit de chercher à faire de la prévention, lors de la mise en place d'outils de *risk management* : les politiques de gestion des risques à court, moyen et long terme dépendent du moment où les risques sont susceptibles d'apparaitre.

La cartographie statistique des risques a permis de mettre en lumière le fait que les risques liés au contrôle et à la maitrise du SI, ceux auxquels on pense de prime abord en évoquant le numérique, ne sont finalement pas les plus importants. Bien connus, ils sont également bien maitrisés, et leur impact est généralement faible dans la vie de l'entreprise. Les principales sources de danger sont plutôt liées au manque de culture numérique au sein de l'entreprise (par les dirigeants comme par les salariés) : ainsi, un défaut de stratégie numérique, une mauvaise gestion des ressources humaines lors du passage au numérique, ou les problèmes liés à la dématérialisation des rapports humains, peuvent entrainer des dommages bien plus importants.

Au cœur des risques liés au numérique, se trouve la problématique de la stratégie numérique : à la fois important facteur de risque, mais aussi premier outil de prévention, la stratégie apparait comme indispensable au bon fonctionnement de l'entreprise numérique. D'autant plus qu'un défaut ou un manque de stratégie peut entrainer d'autant plus facilement la survenue d'autres risques, par exemple juridiques (suite à une mauvaise internationalisation du numérique au sein de l'entreprise), ou marketing (augmentation de la concurrence sur le web). C'est ainsi un nouveau risque qui apparait, intimement relié à la stratégie numérique : le risque systémique, où le numérique devient tellement central dans

l'activité de l'entreprise, dans un système où tout est interconnecté, qu'une défaillance localisée produit des évènements en chaine, et peut entrainer des dommages dans toute la chaine de valeur.

En mettant en parallèle notre rapport avec une réflexion portant sur la révolution numérique de l'entreprise, la stratégie apparait comme un concept clé pour pallier ces risques. Or, si nous avions établi dans un premier temps une définition de l'entreprise numérique très large afin de balayer tout le spectre des risques, il apparait au vu des résultats que cette définition se doit d'être précisée. Les risques stratégiques liés au numérique sont susceptibles d'impacter toute la création de valeur qui en découle. Aussi, le numérique au cœur de l'entreprise n'est créateur de valeur que s'il est stratégiquement implanté. Dans le cadre de la révolution numérique, vue comme une évolution majeure dans les modes de management et d'organisation de l'entreprise au XXI^{ème} Siècle, l'entreprise numérique – par opposition à l'entreprise de management classique – se différencie donc par la volonté « d'être numérique », de tirer profit de la numérisation de son activité. La création de valeur dépend donc d'une politique relative à l'évolution des SI et d'une prise en compte des besoins de l'entreprise et des parties prenantes dans un nouvel environnement. **L'entreprise numérique est finalement une entreprise qui « cherche à tirer une part de sa valeur » du numérique, autrement dit, une entreprise qui possède une stratégie créatrice de valeur quant à la numérisation des ses produits, process ou clients.**

ANNEXES

MÉTHODOLOGIE DE TRAVAIL

Nous avons procédé en suivant une méthodologie de recherche, en quatre étapes :

1. Une phase d'acquisition de connaissances : à partir de documents de réflexion internes au CIGREF, ainsi que d'une bibliographie (voir p. 29), comportant aussi bien des ouvrages que des revues et des articles de presse qui nous a permis d'approfondir les concepts liés aux problématiques du numérique en entreprise.

2. Une phase de reformulation et d'appropriation du sujet : après la phase d'analyse de la littérature, nous avons reformulé le sujet afin qu'il soit correctement appréhendé et défini des hypothèses de recherche pour explorer les différents risques. Bien que relativement courte dans le temps, cette phase a été essentielle pour structurer notre démarche.

3. Une phase d'entretiens avec des professionnels confrontés aux problématiques du numérique : afin d'avoir une approche « terrain », nous avons souhaité recueillir le témoignage et les réflexions de personnes ayant déjà été confrontées aux risques numériques. Nous avons donc élaboré une grille de questions (voir trame d'entretiens en annexes), et nous avons réalisé 6 entretiens semi-directifs.

4. Une phase de traitement et de croisement de l'information, pour aboutir à une typologie des risques, et ensuite une cartographie. Il s'agit de l'étape finale du travail, dans laquelle une certaine simplification a été nécessaire en vue de réaliser une synthèse et une typologie des risques. Après avoir été définis et classés, les risques ont été validés par le CIGREF, puis ils ont été évalués d'après les retours d'expérience des entretiens et la bibliographie. Les conclusions ont été tirées après cette phase de cartographie.

Tout au long de ce travail, les échanges permanents avec les membres du CIGREF ont enrichi et guidé notre réflexion.

Le délai de réalisation de cette étude a été relativement court (8 jours sur 2 mois). Ce travail de recherche mériterait un approfondissement avec une enquête auprès de DSI pour évaluer les risques identifiés, ou l'exploration d'autres modes de cartographie.

NOTATION DE L'OCCURRENCE ET DE LA GRAVITÉ DES RISQUES

Notation obtenue au cours de l'étude.

Famille de risques	Risques	Occurrence	Gravité
Risques RH	Manque d'adhésion/rejet des employés à la politique de numérisation	8	5
	Sclérose du personnel	4	5
	Ralentissement de l'activité de l'entreprise due aux risques sociaux	3	6
Risques éthiques et juridiques	Risque de perte de confidentialité	5	5
	Respect de la vie privée	4	4
	Évolution du droit	4	4
	Imprévisibilité de la justice	3	4
	Internationalisation	6	6
	Perte de la valeur authentique des documents	5	5
Risques liés au contrôle et à la maitrise du SI	Vol/ altération/modification de données de l'entreprise par l'utilisation du système réseau par des employés	3	5
	Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des pirates	2	7
	Vol/altération/modification de données de l'entreprise par l'utilisation du système réseau par des programmes malveillants (virus)	7	3
	Vol/altération/modification de données de l'entreprise suite à la négligence d'un employé	4	3
	Déni de service entraîné par la saturation de réseaux (interne)	3	5
	Déni de service entraîné par la saturation de réseaux (externe)	2	6
	Ralentissement de l'activité de l'entreprise due aux procédures de contrôle	6	3

Risques stratégiques	Conflits internes dus à un défaut de stratégie numérique	7	4
	Perte entraînée par la numérisation d'aspects qui n'auraient pas du l'être (numériser pour numériser)	4	6
	Lock in	6	3
	Concurrence entre des supports de vente	3	7
Risques marketing	Réputation	4	5
	Augmentation de la concurrence	4	6
Risques liés à la dématérialisation des rapports humains	Diminution de la quantité et qualité de la communication	7	4
	Perte de souplesse	8	4
	Réaction plus que réflexion	7	3
	Infobésité	8	3
Risques liés au patrimoine	Conservation (y compris catastrophes naturelles)	4	7
	Valorisation financière	5	6
	Produits non garantis	6	2
Risques périphériques	Risques dus à la perte de contrôle du produit (cf. titrisation)	2	8
	Risques pays (guerre, DDoS, EMP)	1	9

TRAME D'ENTRETIEN

Voici la trame pour les entretiens semi-directifs menés pendant la phase de collecte de données, auprès de DSI et d'autres acteurs de l'IT pour alimenter la réflexion sur l'entreprise numérique et les risques liés.

Les questions subsidiaires permettent éventuellement d'approfondir certains sujets.

Présentation

1) Qui êtes-vous ? En quoi consiste votre travail ?

Le numérique dans l'entreprise

Partie réservée aux interlocuteurs exerçant un métier de DSI (ou autre poste), qui sont à même de parler des problématiques concrètes du numérique dans leur entreprise (ou dans l'entreprise ; ex : consultant).

2) Comment percevez-vous l'évolution du numérique au sein de votre entreprise ces dernières années ?

Questions subsidiaires :

- Votre entreprise cherche-t-elle à développer son potentiel numérique ? / à intégrer de plus en plus le numérique dans ses activités ?
- Si non : pourquoi ?

3) Y a-t-il une réflexion / une politique sur le numérique au sein de votre entreprise ?

Question subsidiaire :

- Si non, pourquoi ?

4) Comment voyez-vous l'évolution future du numérique au sein de votre entreprise ?

L'entreprise numérique

5) Comment définissez-vous l'entreprise numérique ?

6) Quels sont les acteurs de l'intégration numérique d'une entreprise ?

7) Comment voyez-vous l'évolution du rôle de DSI au sein de l'entreprise ?

Les risques et problèmes liés au numérique

8) Quels problèmes concrets avez-vous rencontré dans l'entreprise (à tous les niveaux) au cours du développement du numérique ?

9) Comment réagissent les autres acteurs de l'entreprise à l'intégration du numérique ? (y compris les parties-prenantes)

Question subsidiaire :

- Comment sont gérées les problématiques RH liées au numérique ? (formation des utilisateurs, gestion des compétences…)

10) A quels risques pensez-vous être confrontés aujourd'hui et à l'avenir concernant l'intégration du numérique dans l'entreprise ?

(Plus précisément : sécurité de l'information, cybercriminalité, marketing, juridique, conduite du changement, gestion de l'image, environnement, société, etc.)

Question subsidiaire :

- Comment évaluez-vous ces risques ? Quels sont les plus importants ?

BIBLIOGRAPHIE

Ouvrages

1. ARMSTRONG Jonathan, DRESNER Daniel, RHYS-JONES Mark, *Managing Risk: Technology and Communications*, Butterworth-Heinemann, 2004, 209 p.
2. DE MARESCHAL Gilbert, *La cartographie des risques*, Saint-Denis : AFNOR, collection À savoir, 2003, 50 p.
3. DELAVEAUD Marie-Claude, *Le « Risk Management » en 5 étapes*, Saint-Denis : AFNOR, collection À savoir, 2003, 50 p.
4. DESROCHES Alain, LEROY Alain, VALLÉE Frédérique, *La gestion des risques – principes et pratiques*, Paris : Lavoisier, Hermès Science, mai 2005, 287 p.
5. DUBOIS-MAURY Jocelyne (dir.), *Les risques industriels et technologiques,* Paris : La Documentation française, collection Problèmes politiques et sociaux, novembre 2002, n°882, 120 p.
6. GILLE Laurent, *Les dilemmes de l'économie numérique*, FYP éditions, 2009, 197 p.
7. GODARD Olivier, HENRY Claude, LAGADEC Patrick, MICHEL-KERJAN Erwann, *Traité des nouveaux risques*, Paris : Gallimard, 2002, 620 p.
8. HASSID Olivier, *La gestion des risques*, Paris : Dunod, collection Topos, 2005, 124 p.
9. LEJEUNE Yannick (dir.), *TIC 2025 et les grandes mutations - Comment Internet et les Technologies de l'information et de la communication vont dessiner les prochaines années*, FYP éditions, 2010, 208 p.
10. LICOPPE Christian, *L'évolution des cultures numériques, de la mutation du lien social à l'organisation du travail*, FYP éditions, 2009, 256 p.
11. MÉNARD, Bruno, *L'entreprise numérique. Quelles stratégies pour 2015 ?*, Nuvis, 2010, 155 p.
12. PERETTI-WATEL Patrick, *La société du risque*, 2001, Paris : La Découverte & Syros, collection Repères, 2001, 125 p.

Articles

12. DICKSON Glen, « Post, present and future », *Broadcasting cable*, New York: 6 November 1995, Vol. 125, p. 110-112.
13. KORGAONKAR Pradeep A., KARSON Eric J., "The Influence of Perceived Product Risk on Consumers' e-Tailer Shopping Preference", *Journal of business and Psychology*, Septembre 2007, vol. 22, n°1, p.55-64.
14. DESMEDT Patrice, « Limiter les risques du tout-numérique », *L'usine nouvelle*, 3 septembre 2009, disponible sur internet : http://www.usinenouvelle.com/article/limiter-les-risques-du-tout numerique.N116767.

15. MORLON Jérôme, « L'entreprise étendue : discours ou réalité », *Le Journal du Net*, 7 octobre 2002, disponible sur internet : http://www.journaldunet.com/solutions/0210/021007_faq_extended.shtml.

Publications institutionnelles

16. MINISTÈRE DE L'INTÉRIEUR, « Le guide pratique du chef d'entreprise face au risque numérique », *4e Forum International sur la Cyber Criminalité*, Région de Gendarmerie Nord - Pas de Calais, 31 mars 2010.
17. PROFIL TECHNOLOGY, Le risque numérique vient aussi de l'intérieur – Le livre blanc, disponible sur internet : http://www.profiltechnology.com/fr/pme/profil-network-filter/elements/Livre_Blanc_le_risque_num%C3%A9rique.pdf.

Publications du CIGREF

Les publications du CIGREF sont disponibles sur le site www.cigref.fr