CIGREF

Le rôle de la fonction SI dans la gestion des grands risques

Un exemple avec la Grippe A(H1N1)

Octobre 2010

Synthèse

En matière de gestion des grands risques, la difficulté majeure de l'exercice est la mobilisation générale des acteurs : savoir alerter sans alarmer, se préparer sans trop en faire… Concernant le risque de pandémie grippale H1N1, le virus est très contagieux mais peu mortel, pouvant provoquer un fort absentéisme sur une période de 3 à 4 semaines consécutives en phase aigue.

Face à de grands risques et en période de crise majeure, les Directions des Systèmes d'Information (DSI) agissent en fonction support et doivent, au-delà des impacts possibles dans leurs propres équipes, maintenir et accompagner l'activité des fonctions essentielles de leur entreprise. Dès lors, quel(s) rôle(s) pour les DSI vis-à-vis des Directions Métiers, des Ressources Humaines et de la Direction Générale dans le cas de la survenance d'un grand risque ? Le travail à distance, l'absentéisme des hommes clés, le maintien en condition opérationnelle, la très forte sollicitation des équipes d'assistance et de soutien sont autant d'éléments à préparer. De plus, les SI sont très fortement dépendants des fournisseurs, opérateurs de réseaux, prestataires, intervenants, etc. Il est donc essentiel pour la DSI de pouvoir garantir à la Direction Générale que l'infrastructure générale de l'entreprise sera suffisamment robuste.

La gestion globale de la crise est assurée par les Ressources Humaines (organisation de la distribution des masques et de la logistique, droit du travail, …), la Direction Générale (pilotage de la crise) et les DSI. Ces derniers se concentrent sur des aspects pratiques (adaptation du poste de travail, support à l'organisation de la distribution des masques, PCAs[1], …), dont la fluidité et la gestion reposent particulièrement sur internet et l'organisation du travail à distance. A ce titre, les attentes des Directions Générales vis-à-vis des DSI portent sur les points suivants :

- Maintien du SI en condition opérationnelle ;
- Organisation du travail à distance : certaines DG attendent des DSI qu'ils comblent les carences logistiques de l'entreprise, en termes d'équipement de masques et le travail à distance est un moyen d'éloigner les collaborateurs qui n'ont pas de masques (« masque numérique ») ;
- Sécurité du SI ;
- Support.

Une des missions du CIGREF est d'éclairer et d'alerter les DSI sur les menaces, opportunités, risques qui portent sur la fonction SI, de telle sorte que les entreprises auxquelles ils appartiennent puissent passer ces épreuves dans les meilleures conditions. Cette étude s'attachera donc à analyser et mettre en évidence le rôle du système d'information dans la gestion des grands risques, à travers l'exemple de la Grippe A.

[1] Plans de Continuité d'Activité

Remerciements

Cette synthèse a été réalisée fin 2009, dans le cadre d'une mission confiée par le CIGREF à 3 étudiants HEC dans le cadre de leur cursus de formation de *Master Spécialisé en Management des Risques Internationaux* : Marya Borodina, Sophie Gavenc et Luc Majdalani, sous l'encadrement de Sophie Bouteiller, Chargée de mission au CIGREF.

La méthodologie employée pour réaliser cette étude a été basée sur :

- Des recherches documentaires ;
- Des ressources documentaires issues du CIGREF, notamment des compte-rendus de réunions avec les membres ;
- L'analyse de quelques entretiens menés avec des représentants des entreprises membres, sur la base d'un guide d'entretien (disponible en annexe de cette synthèse).

Ainsi, nous tenons à remercier tout particulièrement les DSI et les *Risks Managers* suivants pour leurs contributions essentielles :

Francis Aaron	Bolloré
Georges Epinette	Stime – Groupement des Mousquetaires
Henri Guiheux	SCOR
Eric Iooss	SFR
Baptiste Maulion	AXA France Services
Eric Veretout	Stime – Groupement des Mousquetaires

Cette étude vise à faire le point sur le rôle de la fonction SI dans la gestion de grands risques tels que la pandémie. Ce document s'adresse en priorité aux DSI et *Risks Managers*, ainsi qu'aux Responsables RH.

Publications CIGREF 2009-2010

- L'architecture d'entreprise dans les Grandes Entreprises
- Cahier de recherche n° 6 : Pratiques et discours des grandes entreprises sur la valeur et la performance des SI - *Etude Exploratoire*
- Communication et influence de la DSI
  Quelle démarche pour une communication au service d'un leadership durable ?
- Les dossiers du Club Achats 2010 : *le point sur … le cloud computing, les audits de licences, l'offshore, les achats IT éco-responsables et l'infogérance*
- Du Green IT aux SI éco-responsables
  2ème édition, augmentée des conclusions du groupe de travail CIGREF 2010
- Impact du Cloud computing sur la fonction SI et son écosystème
  Rapport d'étape et témoignages d'entreprises
- Maturité et gouvernance de l'Open source : la vision des Grandes Entreprises
- Nomenclature 2010 : premier pas vers l'Europe des compétences IT
  Les emplois-métiers du SI dans les grandes entreprises,complété par le référentiel européen des compétences IT
- Le rôle de la fonction SI dans la gestion des grands risques
  Un exemple avec la Grippe A(H1N1)
- Position du CIGREF sur le Cloud Computing
- Relations avec Orange Business Services *(réservé aux membres du CIGREF)*
- Sécurisation de la mobilité

Publications en partenariat

- Audit de la gouvernance des SI (avec l'AFAI et l'IFACI) – A paraître fin 2010
- Les fonctions SI et Organisation au service des métiers (*avec l'AFOPE*) *Optimiser la création de valeur pour l'entreprise*
- L'information : prochain défi pour les entreprises - Pratiques de création de valeur par les SI et leur usage (*avec Capgemini Consulting*)
- Information: the next big challenge for business - Harnessing best practice in IS-driven value creation: 2009 map (*with Capgemini Consulting*)
- SAP Bonnes pratiques commerciales (*avec l'USF*) – A paraître fin 2010

Sommaire

Introduction

A l'ère de la mondialisation, les entreprises doivent faire face à une multiplicité des risques, tous potentiellement imbriqués les uns dans les autres. C'est ainsi que les entreprises, déjà affaiblies par une crise économique et financière majeure depuis la fin 2008, doivent s'organiser pour faire face à une pandémie (réputée sans précédent depuis 40 ans) afin de garantir la continuité de leur(s) activité(s).

Par définition, une pandémie est mondiale : elle touche toute la société, tous les humains, mais ne semble pas, à première vue, concerner la structure même de l'entreprise. Or, si l'entreprise sait gérer l'absence de personnel à titre individuel, elle est mal préparée à le faire pour un nombre plus conséquent de personnes. Elle est encore moins préparée à gérer une crise majeure, d'envergure mondiale, et risquant de paralyser des pans entiers de l'activité économique.

La grippe A est un très bon exemple pour illustrer la nécessaire réactivité de l'entreprise en période de crise. En effet, le premier cas avéré de grippe A date du 18 mars 2009. Trois mois plus tard, l'OMS[2] déclarait officiellement le stade pandémique, en élevant le niveau d'alerte à la phase 6 du Plan mondial OMS de préparation à une pandémie de grippe.

Pour certaines entreprises dites « stratégiques » (fournisseurs d'énergie, télécommunications, …), gérer les grands risques (tels que la pandémie, la crue centennale à Paris, …) est une obligation légale. En effet, elles doivent disposer d'un Plan de Continuité d'Activité réglementaire à jour, dont les différents composants doivent être adaptés à chaque service de l'entreprise. Mais de tels risques, s'ils survenaient, auraient de graves conséquences sur l'ensemble de l'économie d'un pays. C'est pourquoi, en France (comme dans chaque pays), le gouvernement a élaboré un *Plan national de prévention et de lutte « Pandémie grippale »* [3], qui organise la vie et la continuité des activités de la nation en 7 phases. Ce plan s'applique aux citoyens, aux collectivités, aux entreprises, … et définit des règles de gestion sanitaire et organisationnelle visant à limiter les risques de paralysie des activités qui, pour une entreprise, peuvent aller jusqu'au non respect des contrats et des délais de livraison des clients. Au-delà de la notion d'obligation légale, gérer ce type de risque est devenu une condition *sine qua non* en termes d'assurance.

[2] Organisation Mondiale de la Santé

[3] Le plan national de prévention et de lutte « Pandémie grippale » est disponible sur le site officiel : www.pandemie-grippale.gouv.fr

Fin 2009 et début 2010, la gestion du risque pandémique, avec la grippe A, a constitué un excellent exercice pour mettre à jour les PCAs[4] d'entreprises. La démarche a ainsi permis aux entreprises de se préparer au mieux en précisant en amont le rôle du système d'information dans un tel contexte, ainsi que les procédures à mettre en place pendant et après la crise. Le lecteur trouvera dans cette étude une analyse des impacts du risque pandémique sur l'entreprise et du rôle du système d'information dans la gestion de crise.

[4] Plan de Continuité d'Activités

Les impacts d'un risque pandémique sur l'entreprise

L'étude du risque de pandémie

Définition d'une pandémie

Une pandémie se définit selon trois critères : la nouveauté du virus, sa virulence et sa contagiosité.

A titre indicatif, la grippe espagnole, considérée comme une pandémie, aurait touché 40 à 100 millions de personne à travers le monde. Mais, selon les spécialistes, ce n'est pas le pourcentage de personnes infectées qui définit si la maladie est pandémique ou non mais la surface qu'elle occupe. Dans le cas de la « grippe espagnole » (ou « grippe de 1918 »), la Chine fut le premier pays à être touché, suivie par les Etats-Unis, l'Europe puis le monde entier. Les échanges intenses entre les métropoles et leurs colonies furent à l'origine de la diffusion massive du virus. La grippe espagnole aurait, à elle seule, généré plus de morts que la première guerre mondiale d'après certains analystes.

Le ralentissement de l'économie mondiale comme conséquence majeure d'une pandémie

Si la grippe A (H1N1) était de la même gravité que la grippe espagnole, son coût financier s'élèverait à environ 3 000 milliards de dollars selon la Banque Mondiale. La pandémie pose donc un problème majeur pour l'activité économique mondiale, car elle ralentirait considérablement les échanges économiques et les flux financiers.

La première cause de ce ralentissement économique serait le fort taux d'absentéisme en entreprise, et ce de manière simultanée. Ainsi, selon des études officielles de l'OMC[5], dans le cas de la grippe H1N1, 30 à 40 % des personnels pourraient être absents au même moment sur une période de trois semaines en pic de pandémie, puis 15 à 20 % durant 9 semaines sur une période périphérique. Comme le soulignait en mai 2009 le Docteur Keiji Fukuda, Conseiller spécial auprès du Directeur général pour la grippe pandémique à l'OMS, *« A pandemic is a global outbreak. It means that we see both spread of the agent (…) and then we see disease activities in addition to the spread of the virus."*[6]

Les différentes phases de la pandémie grippale selon l'OMS

La propagation du virus au niveau mondial a été suffisamment rapide pour que l'OMS active le niveau d'alerte le plus élevé du *Plan mondial OMS de préparation à une pandémie*

[5] Organisation Mondiale du Commerce

[6] « Une pandémie est une épidémie mondiale. Cela signifie que nous suivons à la fois la propagation de l'agent pathogène et sa virulence, ainsi que la propagation du virus ».

de grippe[7]. En effet, la première phase pandémique de la grippe H1N1 est survenue en mars 2009 à Mexico. Fin avril 2009, l'OMS a relevé le niveau d'alerte à la phase 4, puis à la phase 5 du plan mondial. Mi-juin 2009, l'activation de la phase 6 était annoncée par l'OMS. Cette dernière phase correspond au niveau 5B de notre *Plan national de prévention et de lutte « Pandémie grippale »*. En effet, la France a choisit d'adopter une classification légèrement différente de l'OMS, notamment concernant les phases 5A et 5B.

Phases d'alerte internationale et situations du plan

Phases OMS [1]		**Situations du plan français**
Période à transmission animale prédominante.		
phase 1	Pas de nouveau virus grippal animal circulant chez l'homme	***Situation 1*** Pas de nouveau virus grippal animal circulant chez l'homme
phase 2	Un virus animal, connu pour avoir provoqué des infections chez l'homme, a été identifié sur des animaux sauvages et domestiques.	***Situations 2.*** Épizootie à l'étranger - situation 2A Épizootie en France - situation 2B
phase 3	*Un virus grippal animal ou hybride animal-humain provoque des infections sporadiques ou de petits foyers chez des humaines, sans transmission interhumaine.*	***Situations 3*** Cas humains isolés à l'étranger -situation 3A en France - situation 3B
Période d'alerte pandémique (pré-pandémique)		
phase 4	*Transmission interhumaine efficace.*	***Situations 4*** Début de transmission interhumaine efficace à l'étranger - situation 4A en France - situation 4B
Période pandémique		
phase 5	*Extension géographique de la transmission interhumaine d'un virus grippal animal ou hybride animal-humain.*	***Situations 5*** Extension géographique de la transmission interhumaine du virus à l'étranger - situation 5A en France - situation 5B
phase 6		***Situation 6*** Pandémie
Fin de vague et fin de pandémie		
phases	- post-pic (fin de vague pandémique) : décroissance du nombre des cas dans la plupart des Etats. Possibilité d'une nouvelle vague pandémique ; - post-pandémique : le nombre de cas correspond à ceux d'une grippe saisonnière.	***Situations 7*** Fin de vague pandémique ou fin de pandémie.

Source : Plan national de prévention et de lutte « Pandémie grippale » (4ème édition – 2009, p. 7)

[7] Plus d'informations sur le rôle de l'OMS et les recommandations relatives aux mesures à prendre à l'échelon national avant et pendant une pandémie : http://www.who.int/csr/resources/publications/influenza/FluPrep_F2.pdf

Les mesures gouvernementales de gestion de la crise

Le niveau 6 du plan mondial OMS (correspondant au niveau 5B du plan français), prévoit un taux d'absentéisme de 20 à 40 %. En France, des mesures gouvernementales drastiques pourraient être prises, telles que :

- L'interruption, ou la réduction, de certains transports collectifs locaux, lieux potentiels de transmission du virus, et la restriction du transport aérien de passagers ;
- La suspension des activités collectives : spectacles, rencontres sportives, foires et salons, grands rassemblements, etc. et adaptation des activités cultuelles, restriction des activités professionnelles, sociales, éducatives et associatives non essentielles ;
- La limitation des déplacements individuels aux seuls nécessaires, voire même le confinement de personnels ;
- Des réquisitions ;
- La fermeture des frontières ;
- La fermeture des crèches, établissements d'enseignement et de formation, internats, accueils collectifs de mineurs.

Les entretiens menés dans le cadre de cette étude ont mis en évidence la nécessité de relativiser le risque lié à la pandémie H1N1. En effet, il est peu probable que toute une équipe de salariés soit malade au même moment, et ce durant 9 semaines consécutives. Les absences devraient vraisemblablement se succéder, sans pour autant nécessairement se chevaucher. Cependant, un constat partagé par toutes les personnes interrogées nous permet d'affirmer que se préparer à faire face à cette pandémie, c'est se préparer à faire face à tout type de crise, les risques étant globaux pour l'entreprise.

Les conséquences des mesures gouvernementales sur l'organisation des entreprises

Les conséquences directes

Qu'il s'agisse d'un fort taux d'absentéisme des salariés, ou encore de la baisse des ventes liée à une activité fonctionnant « au ralenti », les conséquences d'une pandémie sur la bonne santé de l'entreprise ne sont pas négligeables. De plus, les mesures gouvernementales prises pour limiter sa propagation peuvent directement impacter l'activité économique du pays et donc l'organisation des entreprises.

Les conséquences des mesures gouvernementales sur l'organisation des entreprises pèsent essentiellement sur les entreprises considérées « d'importance vitale » pour le pays. Selon le décret 2006-212 du 23 février 2006, les *« importances vitales »* correspondent aux activités qui *« concourent à un même objectif, qui sont liées à la distribution et à la*

production de biens et de services indispensables, dès lors que ces activités sont difficilement substituables ou remplaçables ou qui peuvent présenter un danger grave pour la population. ». Ces activités touchent essentiellement les 5 domaines suivants :

- La satisfaction des besoins essentiels pour la vie de la population ;
- L'exercice de l'autorité de l'Etat ;
- Le fonctionnement de l'économie ;
- Le maintien du potentiel de Défense ;
- La sécurité de la nation.

Ainsi, les entreprises stratégiques pour l'économie française doivent répondre à des exigences nationales et sont dans l'obligation de tout mettre en œuvre pour éviter une paralysie de leurs activités, notamment pour permettre à l'Etat d'assurer les siennes.

Les conséquences indirectes

Les conséquences indirectes quant à elles sont définies dans les mesures gouvernementales de réduction de la propagation de la pandémie, notamment au niveau de la phase 5B : fermeture des transports (difficulté pour les salariés de se rendre sur leur lieu de travail), réduction des moyens de garde d'enfants (et par conséquent indisponibilité de personnels qui doivent eux-mêmes garder leur(s) enfants(s)), embouteillages importants ralentissant les déplacements, fermeture des frontières (et problèmes liés à la prise en charge des expatriés).

Si les répercussions de certaines de ces mesures peuvent être acceptables pour l'entreprise, d'autres peuvent être dramatiques dans l'hypothèse où elles touchent des activités critiques pour l'entreprise.

Panorama des enjeux critiques pour une entreprise

Indisponibilité des dirigeants

Les enjeux critiques sont de différents ordres et concernent les moyens dont l'entreprise dispose pour mener à bien son activité. Ils peuvent être tous considérés comme essentiels. La paralysie de l'un des moyens peut entraîner une paralysie totale de l'entreprise. Par exemple, l'indisponibilité simultanée de plusieurs dirigeants, et par conséquent l'incapacité de l'entreprise à prendre des décisions, est un risque envisageable en cas de pandémie. Cela pourrait entraîner d'une part, une paralysie de l'activité et d'autre part, des risques juridiques et économiques pour l'entreprise qui s'engagerait sur de mauvaises stratégies économiques ou qui effectuerait un mauvais management.

Protection sanitaire des salariés

Les salariés, tout autant que les dirigeants, jouent un rôle central pour la survie de l'entreprise : toute la question de la protection sanitaire et de la gestion de l'absentéisme est ici soulevée. Quelle protection offrir aux employés ? Quelle est la responsabilité de l'entreprise face à ses salariés en cas de crise sanitaire ?

Insuffisance énergétique

Pour les entreprises dont l'activité est basée sur l'exploitation de ressources énergétiques (électricité, gaz, pétrole, etc…), toute coupure dans l'approvisionnement de ces ressources pourrait bloquer l'activité et, à terme, menacer la santé de l'entreprise, et évidemment du pays. La pandémie ne peut pas avoir des conséquences directes sur la fourniture d'énergie (laquelle est garantie par les fournisseurs, légalement tenus de disposer des PCAs), mais combinée avec d'autres risques (comme par exemple des risques climatiques), elle pourrait entraîner l'incapacité des équipes techniques des fournisseurs d'énergie (qui fonctionneraient déjà en sous-régime en période de pandémie) à réparer les câbles ou les outils de transmission, risquant ainsi de ne plus alimenter les entreprises en énergie...

Perturbation des télécommunications

Les télécommunications jouent également un rôle central dans la conduite des activités d'une entreprise : sans capacité de communication, la survie de l'entreprise est menacée. La pandémie pourrait indirectement entraîner une saturation des lignes téléphoniques, une surcharge des réseaux de téléphonie mobile et internet, des pannes de serveurs, … La question de la maintenance de ces réseaux et des services d'assistance au consommateur peut être directement mise en avant lors d'une pandémie.

Paralysie des transports

La réduction, voire l'interruption, des transports entraînerait inévitablement des difficultés d'acheminement des biens et des approvisionnements. Le risque majeur dans ce cas porte sur la possible dénonciation des contrats par les clients, qui ne seraient pas livrés dans les délais demandés. Les conséquences économiques pour les entreprises pourraient là aussi être dramatiques.

Défaillance des fournisseurs

La capacité des fournisseurs est un autre problème majeur : en cas de défaut, elle pourrait entraîner une faillite de l'entreprise. Toute la question de l'approvisionnement est ici soulevée. Comment garantir les approvisionnements à ses clients si les fournisseurs font

défaut ? Quel type d'engagement l'entreprise a-t-elle avec eux ? Dans quelle mesure peut-elle les contraindre à remplir leurs engagements ? Et quels sont les garanties dont elle dispose ?

Retrait des actionnaires

L'actionnariat est un élément essentiel de la survie d'une entreprise cotée en bourse. Dès lors, comment rassurer les actionnaires sur la gestion d'une telle crise ? Une mauvaise communication sur les actions menées pour limiter les problèmes pourrait faire fuir les investisseurs…

Pression des agences de notation

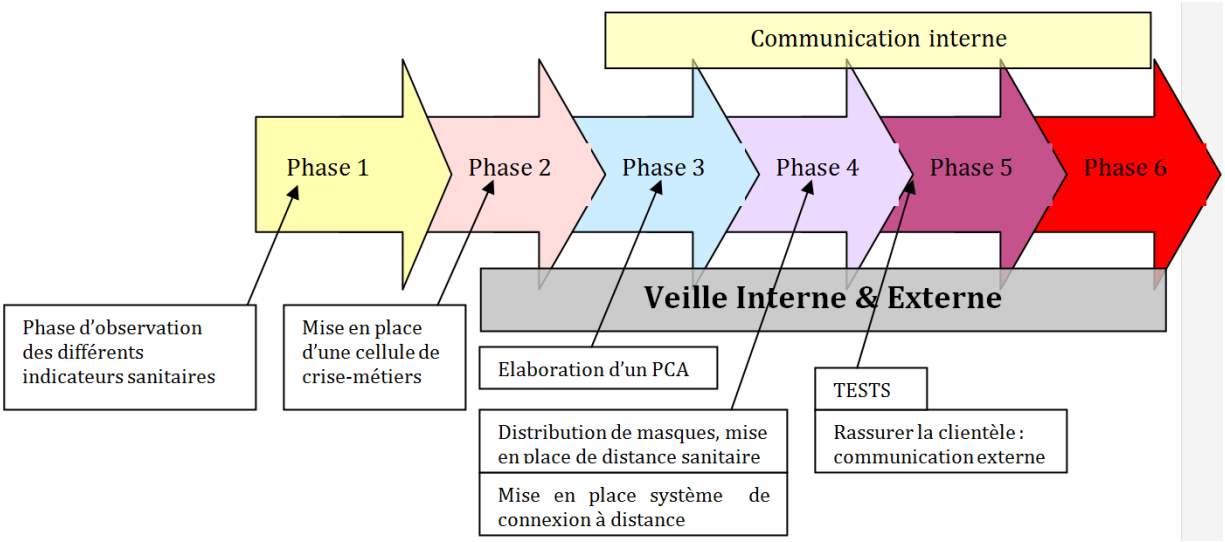
Un dernier point, non moins important, est celui du poids des agences de notation. Des agences comme *Standard & Poor's* par exemple, exigent la mise en place d'un Plan de Continuité d'Activité (PCA) par l'entreprise, son absence pouvant entraîner la baisse de la note de l'entreprise, et par conséquent, une réduction du nombre de contrats avec de nouveaux clients.

Seuil de criticité : intégrité, confidentialité et disponibilité

Il existe une véritable graduation du risque qui rend difficile l'application d'une méthode unique de gestion de crise dans le cas de la grippe A. Ainsi, deux entreprises situées dans des régions différentes pourraient ne pas être placées dans le même niveau de risque. Il convient donc de définir en amont les différentes phases d'acceptabilité et de criticité du risque de pandémie pour chacune des entreprises, en fonction de l'atteinte des services névralgiques de celle-ci.

En effet, le principe même d'une pandémie réside dans la propagation simultanée du virus, il faut donc que l'entreprise définisse des niveaux d'alerte qui amorceront des méthodes de gestion de crise particulières. L'analyse des entretiens menés dans le cadre de cette étude permet de mettre en évidence différentes phases de gestion du risque en fonction des phases sanitaires déclenchées.

Les différentes phases de gestion du risque en fonction des phases sanitaires déclenchées



Source : CIGREF, 2009

La question des seuils

En règle générale, les différentes personnes interviewées lors des entretiens ont révélé qu'elles n'avaient pas envisagé de seuil de déclenchement en fonction des phases annoncées dans le *Plan national de prévention et de lutte « Pandémie grippale »*. En revanche, elles accordent une importance particulière à l'évolution de la pandémie au sein de l'entreprise. Pour cela, elles placent des indicateurs de sensibilité, des « thermomètres », au sein de leur organisation qui leur permettent de réagir de manière mesurée à chaque évolution de situation.

Les seuils de tolérance

Par ailleurs, toutes les interviews ont montré qu'il existe, dans chaque organisation, des seuils de tolérance bien définis. Ils peuvent concerner des aspects juridiques, de sécurité ou économiques, comme par exemple :

- Une implication de l'entreprise pour mauvaise gestion du problème sanitaire et la diffusion d'une mauvaise image pour le groupe ;
- Une convocation aux Prudhommes par un salarié pour mise en danger de la vie d'autrui si aucune mesure de précaution sanitaire n'a été mise en place ;
- Aucune énergie n'est disponible pour faire fonctionner l'entreprise et ses équipements ;
- L'absence de salariés à des postes stratégiques et l'incapacité à effectuer un travail d'importance vitale à distance ;
- La perte de données confidentielles, stratégiques (brevets, licences, …) ;
- L'incapacité de l'entreprise à honorer ses contrats vis-à-vis de ses clients ;

- L'incapacité de l'entreprise à faire transférer les licences des utilisateurs sur d'autres postes ;
- Ou encore de réelles difficultés à se faire livrer par ses fournisseurs.

Approche probabiliste du risque de pandémie

Le tableau suivant propose une méthode décisionnelle en matière de risque pandémique : il montre l'influence des risques causés par la pandémie sur les points clés d'une entreprise, les mesures proposées et le rôle du SI dans le traitement de ces risques.

En utilisant des données diverses, telles que l'expérience de pandémie vécue par les entreprises et au niveau d'un pays (du type grippe aviaire par exemple), les points du PCA, les articles de différents médias, … nous avons tenté d'estimer les probabilités d'occurrence du risque de pandémie et sa gravité. Nous avons segmenté l'aspect probabilité en critères d'occurrence faible, moyenne et élevée.

Les avantages du tableau résident dans sa flexibilité d'utilisation (chaque entreprise peut effectuer une gradation des points clés par importance et développer son propre PCA avec les mesures proposées) et sa simplicité (l'entreprise est représentée au travers d'une alliance d'activités clés, pour lesquelles des menaces sont spécifiquement définies).

Le risque de pandémie : occurrence, impacts business et rôle de la fonction SI

Points clés	Risque	Probabilité d'occurrence	Conséquence sur l'activité	Mesure	Rôle de la fonction SI
Energie	Coupures électriques	Faible	Blocage	Autonomie (générateur, …)	Etablir un plan de consommation optimale d'énergie et réguler la distribution d'énergie en fonction du plan
Télécom-munications	Surcharge	Elevée	Blocage	Autonomie	Sécuriser et protéger les données confidentielles
Transports	Difficultés de livraison et d'approvisionnement	Moyenne	Ralentissements et contrats non honorés	Remplacement, modification des contrat	Identifier les transports prioritaires et optimiser la logistique et les ressources humaines

Points clés	Risque	Probabilité d'occurrence	Conséquence sur l'activité	Mesure	Rôle de la fonction SI
Salariés	Absentéisme	Elevée	Ralentissement / blocage	Travail à distance	Identifier les postes et activités pouvant être assurés à distance, sécuriser les données et assurer la communication en interne
Communication interne	Contagion du personnel et propagation du virus	Elevée	Absentéisme, ralentissement de l'activité, panique du personnel	Imposer des mesures de sécurité	Communiquer sur les mesures de prévention, informer le personnel
Direction	Incapacité des dirigeants à prendre des décisions	Moyenne	Blocage	Délégation de pouvoirs	Adapter les processus de prise de décisions
Distribution	Incapacité des clients à se déplacer dans les points de vente	Moyenne	Baisse des ventes	Développer les canaux de ventes alternatifs	Adapter le SI pour assurer des ventes via le web et livraisons à domicile
Communication externe	Incapacité à échanger avec les pouvoirs publics, et avec les autres entités de l'entreprise	Moyenne	Décisions mal adaptées à la réalité, manque de transparence	Organiser la veille et ???	Mettre en place des canaux de communication adaptés (ligne téléphonique et adresse mail spéciales « Pandémie »)
Protection des données	Intrusion dans le SI / pertes, fuites de données	Elevée	Concurrence, défaut de sécurité	Se renseigner sur les dispositifs prévus par la CNIL, identifier les risques acceptables / inacceptables	Adapter la politique de sécurité au contexte exceptionnel de Pandémie
Fournisseurs	Obligations contractuelles non honorées	Elevée	Ralentissement des activités de l'entreprise, voire blocage	Interroger les fournisseurs sur leur politique de gestion du risque de Pandémie	Adapter les contrats, prévoir la couverture du risque de défaillance du fournisseur

Source : CIGREF, 2009

Le cadre juridique de la gestion de la pandémie

Une entreprise qui ne disposerait pas d'un PCA à jour et testé, et qui ne prendrait pas en compte les consignes gouvernementales, est susceptible de mettre en jeu sa responsabilité civile (qu'elle soit contractuelle ou délictuelle), voire sa responsabilité pénale. En cas de pandémie grippale le service juridique de l'entreprise doit mettre en place différentes mesures.

Les contrats commerciaux

Pour avoir une vision claire des conséquences d'une pandémie dans l'hypothèse où l'entreprise ne serait pas en mesure de remplir ses obligations contractuelles, le service juridique doit indiquer aux dirigeants les risques juridiques, et les sanctions contractuelles notamment, découlant du non respect des engagements de l'entreprise vis-à-vis de ses clients. Une fois ces risques identifiés, le service juridique doit proposer des solutions : adaptation des contrats, renforcement des contrats d'assurance, insertion d'annexes au contrat concernant les cas de force-majeur, ou possibilité de signer un contrat avec un nouveau fournisseur.

Les cas dits de « force majeure » (charge à chaque interlocuteur de les définir en situation de crise, car dans l'article 1148 du Code civil, aucune pré qualification n'est mentionnée) peuvent être utilisés dans les contrats commerciaux, en respectant les règles de :

- L'irrésistibilité : l'évènement est insurmontable ;
- L'imprévisibilité : le débiteur qui n'a pas pris les mesures nécessaires est en faute ;
- L'extériorité : si l'événement est imputable à une partie, celle-ci engage sa responsabilité ; le débiteur ne peut invoquer la défaillance de son personnel, de son matériel ou de la technique utilisée ;
- Les relations avec le personnel (les relations juridiques internes).

La responsabilité de l'employeur en matière de sécurité

La Direction des Ressources Humaines, en liaison avec le Médecin du Travail et le CHSCT[8], doit évaluer les risques de la pandémie pour la sécurité et la santé des travailleurs. Elle doit les retranscrire dans un document unique d'évaluation des risques (DUER), communiqué à l'ensemble des salariés. L'absence de mise à jour de l'évaluation des risques est passible d'une contravention de cinquième classe (7.500 € pour une entreprise, 15.000 en cas de récidive).

[8] Comité d'Hygiène, de Sécurité et des Conditions de Travail

En France, en cas de passage aux phases 5B voire 6 du *Plan national de prévention et de lutte « Pandémie grippale »*, il est fort probable que certains salariés, voulant éviter la contagion, invoquent le droit de retrait. Dans cette hypothèse, le salaire de la personne doit être intégralement maintenu. Toutefois, comme le souligne la circulaire DGT (DGT 2007/18 du 18 décembre 2007) « sous réserve de l'interprétation souveraine des juges, ce droit ne pourra être exercé que de manière exceptionnelle si l'employeur met en œuvre les mesures de prévention et de protection adéquates. ».

La question des laissez-passer

Dans le cadre des phases 5B et 6, le *Plan national de lutte et de prévention « Pandémie grippale »* prévoit la mise en place de « mesures barrières de freinage et de limitation d'extension de la maladie ». Afin d'anticiper ce risque, l'entreprise peut transmettre à la Préfecture et aux services de police auxquels elle est rattachée, la liste des personnels clés afin d'obtenir les laissez-passer nécessaires. Toute mesure restrictive de la Préfecture concernant la circulation de la population sur son territoire peut en effet largement entraver l'activité des entreprises situées dans cette zone.

Cette décision peut également s'accompagner d'une restriction / limitation des activités professionnelles, sociales, éducatives ou associatives non essentielles. Dans ce cas, le travail à distance est indiqué comme l'une des possibilités permettant de maintenir les activités essentielles de l'entreprise.

L'encadrement juridique du télétravail

L'encadrement juridique du télétravail est loin d'être clair. A la lecture de la législation relative au travail, si le télétravail demeure soumis à l'accord préalable du salarié, il reste que cette décision est réversible. Dans certains cas, le refus du salarié peut constituer une faute. En effet, selon l'article L 12 33-1 du code du travail, l'employeur peut décider unilatéralement de changer les conditions d'un contrat en cas de pandémie (heures supplémentaires, augmentation des tâches, …). Dans le cas d'une modification de cette nature, l'employeur est tenu de mettre en place une procédure de notification avec LRAR[9] et d'accorder au salarié un délai de réflexion « raisonnable ».

Pour cette raison, de nombreuses entreprises ne parlent pas de « télétravail » mais de « solution temporaire de travail à distance due à une situation exceptionnelle de pandémie » ou plus simplement de « travail à distance ».

[9] Lettre Recommandée avec Accusé de Réception

La protection des données confidentielles de l'entreprise

Dans l'hypothèse de la mise en place du travail à distance, plusieurs points doivent faire l'objet d'une analyse de risques :

- La gestion des accès ;
- La gestion des identifications au système d'information de l'entreprise ;
- Les mesures de sécurité à prendre sur le poste de travail du collaborateur ;
- L'assurance de l'entreprise.

Le service juridique, en liaison avec la DRH, doit indiquer les risques auxquels l'entreprise s'expose dans le cadre de la mise en place de cette solution, notamment pour ce qui concerne les flux d'information (article 226-17 du Code Pénal – le délit de manquement à la sécurité du système d'information), et la sécurité des donnés personnelles des employés (L. 121-8 du Code du travail – aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été préalablement porté à sa connaissance). En cas d'externalisation d'activités auprès d'un prestataire (hébergement, sauvegarde/secours), le contrat le liant au client devra prévoir des clauses spécifiques pour poursuivre son activité même en présence d'un sinistre (physique ou informatique) ou d'une crise sanitaire et sociale.

Le rôle du Système d'Information (SI) dans la gestion de la crise

Le Plan de Continuité d'Activité (PCA)

La gestion du risque de pandémie permet de mettre en place des mesures de sécurité et de continuité d'activité adaptées à d'autres facteurs de risques : attaques chimiques, bactériologiques, catastrophes naturelles, paralysie ou destruction d'infrastructures vitales, … C'est une sorte de simulation grandeur nature, une « opportunité » en termes de gestion de risques/crises. Les entreprises stratégiques ont le devoir d'établir un PCA selon l'article L4121-1 du code du travail. Pour les autres entreprises, il est vivement conseillé d'en définir un et de le tester, puisqu'en cas de crise, l'employeur est tenu de prendre les mesures nécessaires pour assurer la sécurité du personnel et d'évaluer les risques au travers d'un PCA.

De l'utilité d'avoir un PCA…

Le PCA comprend l'élaboration de consignes de sécurité et de protection, l'acquisition d'équipements et de matériels d'hygiène (masques, solutions hydro-alcoolisées, …), définit les procédures de mise en place des freins à la contagion (accès des locaux, nettoyage, hygiène, informations via des affichettes, …) et la mise en œuvre de mesures préparatoires. L'efficacité des mesures est fonction de leur appropriation par le personnel : il ne faut donc pas hésiter à communiquer sur le PCA et le tester avec les salariés.

Le PCA est le fer de lance de la gestion du risque pandémique : il doit permettre, autant que possible, de faciliter la circulation de l'information au sein des différents services de l'entreprise et de maintenir un fonctionnement efficace et transparent, en coopération avec les autorités.

L'élaboration d'un PCA

Créer une cellule de crise et nommer un responsable « Pandémie grippale »

Il est indispensable d'identifier les postes clés de l'entreprise, de les protéger, et de déterminer une solution de secours en cas de vacance d'un poste. C'est un des rôles de la cellule de crise (ou du comité d'alerte), qui garantit que les décisions importantes seront prises de manière centralisée. La cellule de crise doit également déterminer quelles sont les missions qui doivent être assurées en toutes circonstances. Cette tâche relève généralement de la responsabilité du Responsable « Pandémie grippale », dont le rôle est aussi de prévoir des modes d'archivage et des procédures de « *back-up* » dans le PCA.

Respecter les normes en vigueur

Le PCA doit répondre à certaines normes, variables d'un pays à l'autre :

- Norme Afnor BPZ 74-700 – France
- Norme NFPA 1600-20043 – Etats-Unis
- Guides BSI OAS 56 et BSI PAS 25999 – Royaume-Uni

D'un point de vue juridique, il est tout à fait possible qu'une entreprise décide d'externaliser la mise en place de son PCA. Il est important de négocier les clauses du contrat en définissant notamment les « prestations essentielles », à savoir la sauvegarde de l'ensemble du patrimoine de l'entreprise, et ce jusqu'à la reprise normale de l'activité. Ceci devra bien évidemment être effectué dans le respect de la confidentialité des informations relatives au personnel de l'entreprise.

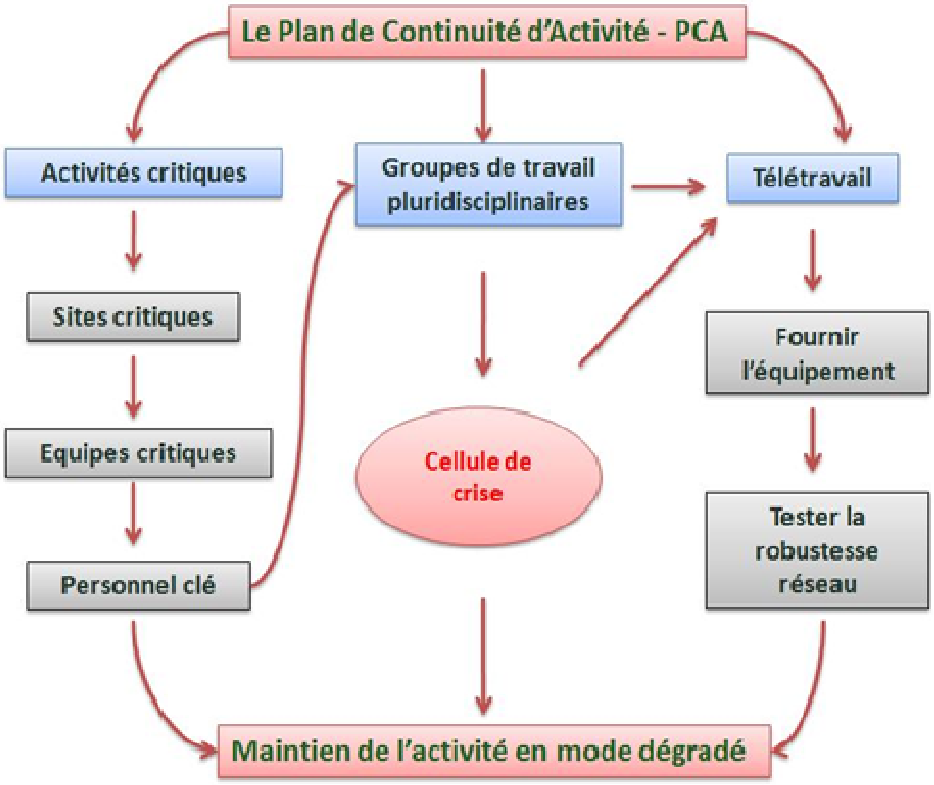
De surcroît, la question probable en cas de pandémie est celle des besoins vitaux de l'entreprise : énergie, communication, transport, eau potable, etc. Il est impératif de maintenir ces besoins à un niveau acceptable, le PCA doit donc y veiller. il faut s'interroger sur la question de l'approvisionnement, indispensable à la production. Il faut être en accord avec les fournisseurs et sous-traitants sur les conditions d'approvisionnement et de livraison en mode dégradé. En cas de manquement de leur part, il serait judicieux d'avoir une ou plusieurs alternatives.

Les points essentiels du PCA

Le PCA doit :

1. Identifier les missions à maintenir et celles à suspendre (provisoirement) ;
2. Identifier les personnels clés ;
3. Définir les ressources nécessaires au maintien des activités (en mode dégradé) ;
4. Concernant les Ressources Humaines :
   - Sélectionner et dimensionner les postes qui participent aux processus critiques ;
   - Développer la polyvalence, constituer un vivier d'inactifs activables ;
5. Au niveau technique
   - Développer le travail à distance ;
   - Développer les canaux de vente alternatifs (web, …) ;
   - Adapter la politique de sécurité SI
6. Mettre en place une cellule de crise : information, communication, veille et alerte
7. Identifier des correspondants locaux dans les pays où sont implantées des filiales
8. Préparer les outils et moyens de communication
9. Permettre le maintien des relations avec toutes les parties prenantes de l'entreprise en France et à l'étranger.

Plan de Continuité d'Activité : proposition d'organisation



Source : CIGREF, 2009

Une entreprise qui ne dispose pas d'un PCA, à jour et testé et qui ne prend pas en compte les consignes gouvernementales, est susceptible de mettre en jeu sa responsabilité civile, voire pénale.

Les étapes de la gestion du risque par le SI : la fonction SI doit s'organiser et accompagner l'entreprise dans la mise en place du PCA

Maintenir le SI en condition opérationnelle

Dans l'hypothèse d'un absentéisme de 20 à 40% des effectifs durant la période de crise la plus aigue (projections de l'OMS et des pouvoirs publics français), les effectifs informatiques peuvent être touchés. Il faut donc prévoir de remplacer les postes essentiels :

- Dresser une liste des fonctions clés de la DSI et prévoir leurs remplacements (doublement des équipes, *back up*) ;
- S'assurer que les remplacements sont prévus à 2 niveaux :
  - Un remplaçant installé dans un bureau différent de la personne clé mais situé sur le même site ;
  - Un remplaçant installé sur un site éloigné d'au moins 100 km ;

- En cas d'aggravation extrême de la situation pandémique, les déplacements sur le territoire national seront fortement limités (cf. pages 60 et 61 du *Plan national*) : dans ce cas (peu probable), il pourra être utile de transmettre la liste des personnels clés à la Préfecture de manière à obtenir les laissez-passer nécessaires.

Maintenir le SI en condition opérationnelle signifie aussi de s'assurer que les fournisseurs seront en capacité d'assurer leurs obligations contractuelles vis-à-vis de leurs clients. Sur ce point, fin 2009, les DSI semblaient davantage préparés que les fournisseurs. En effet, certains DSI ont envoyé des lettres à leurs fournisseurs stratégiques pour savoir comment ceux-ci se sont préparés au risque de pandémie. Ce qu'il ressort des réponses fournies pointe le fait que les fournisseurs n'ayant pas d'obligations légales vis-à-vis de leurs clients, beaucoup feront leurs *best efforts* et sont incapables d'assurer à leurs clients qu'ils seront en mesure d'assurer le service. Par ailleurs, certains fournisseurs invoqueront certainement le cas de force majeure. Cependant, la pandémie pouvant être anticipée, cet argument n'est pas recevable et les fournisseurs seront donc tenus de respecter leurs engagements contractuels. Concernant les fournisseurs d'énergie et les opérateurs, ceux-ci disposent de 2 types de PCA : l'un, réglementaire, sera mis en place si le niveau 6 du Plan national « Pandémie grippale » est déclaré ; l'autre, PCA intermédiaire, doit permettre d'assurer le service pour tous les clients.

Faciliter la veille

Les responsables de la gestion de crise doivent pouvoir s'informer très régulièrement sur l'évolution de la situation (localement et globalement) : dépêches d'actualité, presse, internet, … Ils doivent pouvoir aussi communiquer entre eux, informer la DG, les responsables de sites locaux, détecter toute modification du cadre réglementaire :

- Donner accès aux outils de veille ;
- Assurer la mobilité avec les outils appropriés (accès aux flux vidéo notamment).

Permettre la communication interne et externe de l'entreprise

La situation de pandémie génère beaucoup de tensions et d'angoisses et la communication interne revêt alors un caractère particulièrement stratégique et essentiel. En matière de SI, ce point se traduit par :

- La mise en place d'un intranet dédié à la pandémie, point de contact et d'information unique pour tous les salariés qui souhaitent s'informer sur le sujet : mise à jour fréquente, informations pratiques sur les mesures sanitaires, recommandations aux voyageurs ;
- La mise en place d'un extranet pour faciliter la circulation des informations, notamment pour les salariés qui travaillent depuis leur domicile ;

- L'organisation de la communication entre le siège de l'entreprise, les correspondants locaux dans chaque pays et les autorités publiques internationales (OMS) et locales (hôpitaux, Consulats / Ambassades, Ministères des Affaires Etrangères / de la Santé).

Mettre en place des solutions de travail à distance, tester les applications stratégiques et la robustesse des moyens d'accès

Le niveau 6 de l'alerte OMS implique le déclanchement de dispositions visant à freiner la propagation de la maladie (fermeture des écoles, restrictions d'accès aux transports en commun, recommandations de « distanciation sociale », …). Pour anticiper ce risque, la fonction SI doit prévoir l'activation des dispositifs de travail à distance, tel que le télétravail[10]. Cependant, la notion de télétravail pose d'importants problèmes juridiques pour l'entreprise, tant en termes de mise à disposition du matériel (ligne ADSL, téléphone, ordinateur, …), qu'en termes d'assurance. Le cadre normatif autour du télétravail étant très complexe (implications des Instances Représentatives du Personnel, relations avec la CNIL, …), certains DSI parlent de « solution temporaire de travail à distance due à une situation exceptionnelle de pandémie », en accord avec les RH. Pour les personnels clés qui auraient laissé leurs matériels au bureau (ordinateurs portables, terminaux mobiles *blackberry*, …), certaines entreprises ont prévu des systèmes de livraison à domicile. Cependant, compte tenu des difficultés et de la complexité de la mise en place de telles solutions, la fonction SI doit également veiller à informer les directions utilisatrices des possibilités réelles et raisonnables en matière de travail à distance, et concentrer ses efforts sur les besoins à caractère impératif et stratégique.

Par ailleurs, pour anticiper le risque d'absentéisme, certains DSI ont mis en place, via leur intranet, un outil d'auto-déclaration et/ou de suivi des congés. Cependant, le site web, ou encore la messagerie sont aussi des outils possibles pour anticiper le risque d'absentéisme et déclarer les absences. Le plus difficile en matière d'absentéisme sera de gérer les réactions individuelles et collectives des salariés : on ne peut pas les anticiper, et on ne les maîtrise pas. Par ailleurs, il est vraisemblable que les entreprises ne pourront pas faire autrement que d'imposer à leurs collaborateurs absents mais non malades (garde d'enfants, absence de transports, …) de poser des congés et des jours de RTT.

Enfin, tester les applications stratégiques et la robustesse des moyens d'accès au SI de l'entreprise implique pour la fonction SI de préparer l'arrêt de certaines applications, exercice difficile mais essentiel. La fonction SI doit travailler avec les Métiers pour identifier

[10] Le *télétravail* se définit comme « une forme d'organisation et/ou de réalisation du travail, utilisant les TIC dans le cadre d'un contrat de travail et dans laquelle un travail, qui aurait également pu être réalisé dans les locaux de l'entreprise, est effectué hors de ces locaux de façon régulière. » (Art. 1er de l'accord national interprofessionnel du 19/07/2005).

les processus critiques du *business*. Certains DSI l'ont fait, d'abord seuls, puis avec les Métiers. Il en ressort qu'il est possible de modifier les processus, mais qu'on ne peut pas tout bouleverser, les Métiers doivent donc jouer le jeu de leur côté.

Assurer la sécurité des systèmes d'information autant que possible

La sécurité des systèmes d'information est un enjeu majeur, mais en période de crise, la politique de sécurité doit être adaptée. Pour la fonction SI, cela se traduit par un travail conjoint avec le RSSI[11] pour :

- Adapter les conditions d'accès à la mobilité (délégations de pouvoir étendues pour certains collaborateurs, ...) ;
- Réviser et adapter les chartes informatiques pour assouplir temporairement les règles (pas de renouvellement des mots de passe par exemple, politique du compromis, relecture de la politique de sécurité sur les accès distants, …).

De plus, dans le cadre du travail à distance, il y a un réel risque de perte / fuite de données, ainsi qu'un risque élevé d'intrusion. Il faut s'attendre à voir les taux de disparition et de sortie de données bien au-dessus de ce que l'on a l'habitude de voir (données critiques). La question à se poser est la suivante : est-on prêt à accepter que quelqu'un puisse prendre la main sur un poste à distance ?

Interroger les sous-traitants informatiques sur leur organisation et leur niveau de préparation en cas de pandémie

La préparation à la continuité d'activités des entreprises doit comprendre une démarche vers les sous-traitants informatiques pour connaître leurs plans de continuité d'activités et les services qui pourront être assurés. Les 2 questions à leur poser sont :

- Avez-vous prévu une organisation spécifique en cas de pandémie et si oui, laquelle ?
- Comment avez-vous traité ce risque, avez-vous adapté et testé votre Plan de Continuité d'Activités ?

[11] Responsable de la Sécurité du Système d'Information

Conclusion

Que ce soit pour des raisons réglementaires, économiques ou structurelles, les entreprises devront trouver les moyens de gérer les grands risques tels que la pandémie grippale. Les enjeux sont élevés, allant d'un simple ralentissement de l'activité de l'entreprise à une véritable paralysie de l'économie qui pourrait, dans certains cas, entraîner des dommages non négligeables en termes de pertes financières. Au-delà des enjeux financiers, l'entreprise (qu'elle agisse dans un secteur stratégique ou non) peut être juridiquement mise en cause en cas de mauvaise préparation au risque pandémique.

Même si le risque de pandémie ne se gère pas de la même manière dans toutes les entreprises, ni même dans tous les pays, le meilleur moyen d'anticiper ce risque et d'en limiter les impacts sur l'entreprise est le PCA, dont le SI est l'outil privilégié. Les points à retenir concernant l'organisation de l'entreprise et le rôle de la fonction SI dans la gestion de la crise sont les suivants :

- Maintenir le SI en condition opérationnelle : la préparation de l'arrêt de certaines applications non critiques pour l'entreprise est un exercice difficile mais essentiel, il faut y travailler avec les Métiers ;
- Faciliter la veille ;
- Permettre la communication interne et externe de l'entreprise ;
- Mettre en place des solutions de travail à distance, tester les applications stratégiques et la robustesse des moyens d'accès ;
- Assurer la sécurité des systèmes d'information autant que possible, notamment dans le cadre du travail à distance (envisager le risque d'intrusion et de perte / fuite de données sensibles et donc adapter la politique de sécurité) ;
- Interroger les sous-traitants informatiques sur leur organisation et leur niveau de préparation en cas de pandémie, car les fournisseurs ont des obligations contractuelles vis-à-vis de leurs clients ;

Enfin, il faut nuancer les conséquences possibles du risque pandémique. Les mesures gouvernementales de limitation de la propagation mises en œuvre au nom du principe de précaution peuvent paraître quelque peu démesurées par rapport à la gravité réelle de la situation. En effet, pour gérer le risque toujours d'actualité de pandémie de grippe A, le gouvernement a mis à jour le plan élaboré en 2006 pour gérer le risque de grippe aviaire, virus extrêmement mortel et contagieux (contrairement à celui de la grippe A tel que nous le connaissons aujourd'hui). Dès lors, pour gérer ce risque, les entreprises sont contraintes de mettre en place un PCA parfois trop restrictif. Néanmoins, les entreprises interrogées dans le cadre de cette étude sont unanimes : la gestion du risque de pandémie est une préparation optimale et adaptée à la gestion des grands risques.

Annexe : Les méthodes de prévention du risque pour les SI

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en France, portail gouvernemental de la sécurité informatique (www.ssi.gouv.fr), est l'organisme interministériel officiel définissant les normes de la sécurité des systèmes d'information, en particulier les normes sur l'évaluation et la certification des SI.

La méthode EBIOS

L'ANSSI a développé la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), qui permet à une entité d'apprécier et de traiter les risques relatifs à la sécurité de ses systèmes d'information, de communiquer en interne et vis-a-vis de ses partenaires, afin de contribuer au processus de gestion des risques en prenant en compte toutes les entités techniques (logiciels, matériels, réseaux) et non techniques (organisation, aspects humains, sécurité physique).

La méthode EBIOS est largement utilisée dans le secteur public (l'ensemble des ministères et des organismes sous tutelle), dans le secteur privé (cabinets de conseil, petites et grandes entreprises), en France et à l'étranger (Union européenne, Québec, Belgique, Tunisie, Luxembourg…), par de nombreux organismes en tant qu'utilisateurs ou bénéficiaires d'analyses de risques SSI. Sa diffusion est gratuite sur le site de l'ANSSI.

Cette méthode permet de construire une politique de sécurité en fonction d'une analyse des risques reposant sur le contexte de l'entreprise et des vulnérabilités liées à son SI. La démarche est commune à tous, mais les résultats de chaque étape sont personnalisés. EBIOS étudie le contexte, les besoins, les menaces, les objectifs ainsi que les exigences de sécurité.

L'étude du **contexte** a pour objectif d'identifier globalement le système-cible et de le situer dans son environnement au travers de trois activités :

1. Une étude de l'organisme : cette activité consiste a définir le cadre de l'étude. Il faut collecter les données à son sujet sur son système d'information ;
2. Une étude du Système Cible : afin de préciser le contexte d'utilisation du système à concevoir ou existant ;
3. La détermination du périmètre de l'étude pour connaître les entités sur lesquelles vont reposer les éléments essentiels du système-cible.

L'étude des **besoins** se divise en trois activités :

1. La sélection des éléments sensibles ;

2. La détermination des fiches de besoins afin de créer les tableaux nécessaires à l'expression des besoins de sécurité par les utilisateurs ;
3. La synthèse des besoins de sécurité : pour attribuer à chaque élément essentiel les besoins de sécurité.

L'étude des **menaces** se divise en quatre activités :

1. L'étude des origines des menaces (menaces génériques) : correspondant à l'identification des sources dans le processus de gestion des risques ;
2. L'étude des vulnérabilités pour déterminer des points faibles spécifiques du système-cible ;
3. L'étude des risques spécifiques afin de disposer d'une vision objective des menaces pesant sur le système-cible ;
4. Et la confrontation des risques aux besoins pour retenir et hiérarchiser ceux qui sont véritablement susceptibles de porter atteinte aux besoins.

L'étude des **objectifs** de la sécurité se divise en deux activités :

1. La détermination des niveaux de sécurité servant à déterminer le niveau de résistance adéquat pour les objectifs de sécurité. Ce qui permet également de choisir le niveau des exigences de sécurité d'assurance.
2. La formalisation des objectifs de sécurité pour déterminer les objectifs de sécurité permettant de couvrir les risques.

L'exigence de sécurité concerne la spécification des mesures concrètes à mettre en œuvre pour traiter les risques sur la base d'une négociation argumentée.

L'étude des menaces est un recensement des scénarios pouvant porter atteinte aux composants (techniques ou non) du SI. Cette étude consiste en un recensement des scénarios pouvant porter atteinte aux composants du SI. Une menace peut être caractérisée selon son type (naturel, humain ou environnemental) et/ou selon sa cause (accidentelle ou délibérée).

La méthode EBIOS a beaucoup d'avantages. C'est une méthode claire qui fournit des informations objectives sur les acteurs, leurs rôles et leurs interactions. Son approche est exhaustive, contrairement aux approches d'analyse des risques par scénarios. La démarche structurée de la méthode EBIOS permet d'identifier les éléments constitutifs des risques. De plus, la méthode EBIOS peut être adaptée au contexte de chacun et ajustée à ses outils et habitudes méthodologiques grâce à une certaine flexibilité. Les exigences de sécurité seront déterminées afin de spécifier des mesures de sécurité, mais leur mise en œuvre sera réalisée à la suite de l'étude. Cette méthode ne fournit pas de recommandations ni de solutions immédiates aux problèmes de sécurité.

Le référentiel MEHARI

Le référentiel MEHARI, quant à lui, a été conçu pour aider les RSSI[12] sur les sujets relatifs au management et à la sécurité des SI. MEHARI est un référentiel méthodologique dont la conception est basée sur une base de connaissances, visant à aider les dirigeants et les responsables d'entreprises dans leurs actions et processus ainsi que les acteurs pouvant réduire les risques.

Il existe deux modules de diagnostic dans l'ensemble MEHARI :

- Un module de diagnostic rapide.
- Un module de diagnostic approfondi.

MEHARI propose un module d'analyse des enjeux, qui débouche sur deux types de résultats :

- Une classification des dysfonctionnements par niveau.
- Une classification des informations et ressources du système d'information.

La classification des dysfonctionnements est une démarche structurée, qui recherche les dysfonctionnements opérationnels à partir de l'activité de l'entreprise pour :

- Mesurer la gravité des paramètres de chaque dysfonctionnement ;
- Décrire les types de dysfonctionnements redoutés ;
- Bien évaluer les seuils de criticité de ces paramètres qui font passer la gravité des dysfonctionnements d'un niveau à un autre.

MEHARI propose une approche structurée du risque qui repose sur quelques éléments simples. Une situation critique, où le niveau de risque est assez élevé, est caractérisée par :

- Des facteurs structurels liés à l'activité et au métier de l'entreprise, et qui ne dépendent pas des mesures de la sécurité ;
- Des facteurs liés aux mesures de sécurité mises en place.

Les normes internationales

Le management de la sécurité des systèmes d'informations au niveau européen passe par des certifications et des normes sélectionnées par la Commission Européenne, qui visent à renforcer la sécurité des systèmes d'informations dans les 27 Etats membres de l'Union Européenne (UE).

[12] RSSI : Responsables de la Sécurité des Systèmes d'Information

Pour la protection et la sécurité de leurs systèmes d'information, les entreprises sont désormais tenues de respecter :

- Soit la norme ISO/CEI 27002 : il s'agit d'un ensemble de 133 mesures ayant pour objectif d'instaurer des règles de sécurité et de contrôle pour tous types de systèmes d'information. Ces mesures indiquent uniquement les thèmes et les points importants devant être adoptés mais pas la manière de le faire. C'est aux entreprises de savoir comment les mettre en place selon leurs besoins. Ces mesures sont donc d'une grande flexibilité et sont issues des « bonnes pratiques » et de l'expérience d'un grand nombre d'entreprises.
  Plus d'informations : www.iso.org

- Soit la certification allemande du BSI, composé de trois grands chapitres qui s'occupent:
  - De la sécurité des applications, de celle des infrastructures essentielles et d'Internet
  - De la cryptographie et de la lutte contre l'écoute clandestine
  - De la certification, de l'approbation et de l'évaluation de la conformité ainsi que de l'étude des nouvelles technologies

  Plus d'informations : www.bsi.de

- Soit l'outil de gouvernance des SI, CobiT. La Communauté Européenne a décidé en 2004 d'adopter CobiT, comme nouvelle norme de sécurité pour les systèmes d'information de ses organismes payeurs. CobiT est un outil de gouvernance des systèmes d'information, qui cherche à automatiser un grand nombre de fonctions dans l'entreprise. Il aide à comprendre et à gérer les risques et les bénéfices qui leur sont associées pour que celles-ci deviennent des centres de profits et de performance. Il s'aligne directement avec les métiers de l'entreprise.
  Plus d'informations : www.isaca.org