A N D S I

Association Nationale des Directeurs des Systèmes d'Information

www.andsi.fr

La gestion de crise et la continuité d'activité

Compte rendu de la présentation du 10 juin 2014 à l'Ecole Militaire

Compte rendu rédigé par Isabelle MAURANGES & ANDSI

En bref…

Ce soir J-L WYBO et E WIATROWSKI présentent deux visions de la gestion de crise. Le premier insiste sur des prérequis indispensables, notamment sémantiques, et le second intervient sur son vécu terrain …

Pour M. WYBO, ''Attention'' n'est pas ''Vigilance'' et gérer la crise n'est pas gérer l'urgence car l'urgence implique l'existence de risques de dommages prévisibles quand la crise provoque avant tout une déstabilisation de l'organisation. Pour réussir la gestion de crise, construisons collectivement et coopérons efficacement.

Pour M. WIATROWSKI, les politiques de continuité d'activité de son entreprise arrivent de la maison mère, puis se déclinent par entités. Chaque activité est doublée et back-upée sur un autre site. La continuité s'implémente au niveau local puis alimente la continuité d'activité globale. La continuité sert prioritairement à la sauvegarde de l'image de l'entreprise et au maintien de ses parts de marché. Pour gérer la crise, manageons l'improbable avec flexibilité en nous appuyant sur les REX ou RETEX (pour retour d'expérience) et osons prendre les décisions toujours difficiles !

Exposé de M. Jean-Luc WYBO

Mines ParisTech – PSL Research University

Jean-Luc WYBO, tout en nous rappelant quelques « basics », met l'accent sur la prévention des crises.
La plupart des méthodes d'analyse de risques ont une approche cartésienne donc de systèmes « compliqués », décomposables en unités simples. Or, la plupart des systèmes réels sont « complexes » (non décomposables) ; il est donc nécessaire d'interpréter les situations suivant les trois axes de la complexité :

- **La technologie** dont on ne sait pas toujours contrôler les processus, les dynamiques et les interactions ;
- **Les acteurs et les utilisateurs** qui, avec leurs différences de perception, imposent des injonctions contradictoires que vous n'imaginiez pas et qui nuisent à votre compréhension ;
- **L'organisation, enfin,** qui ne dit pas si elle se base sur le respect de la règle ou sur l'autonomie maîtrisée de ses cadres et/ou employés.

Mais pourquoi interpréter ? Pourquoi analyser systèmes et situations de risques ? Trois principales raisons :

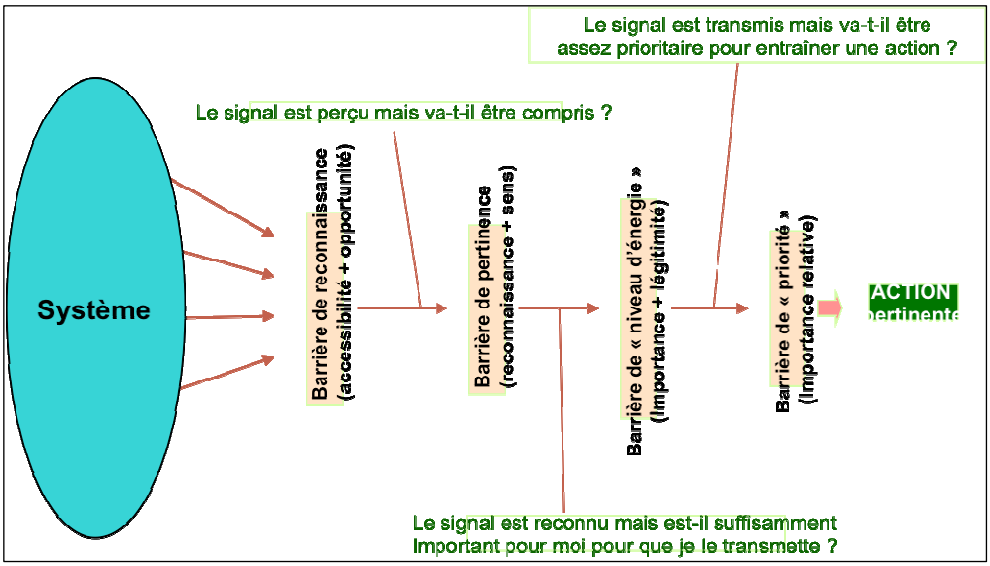
- Pour donner du sens et expliquer ce que sont ces risques ;
- Pour trouver un équilibre entre le concepteur qui crée le système ou la procédure et l'opérateur qui l'utilise au quotidien sur le terrain ;
- Pour trouver le bon dosage entre la rigidité nécessaire *(exemple des procédures de fabrication de médicaments)* et les degrés de liberté à laisser *(exemple de la surveillance policière ou de la maintenance).*

Il faut bien distinguer ''attention'' et ''vigilance'' : si l'on précise ''quelque chose'' à surveiller, nous y prêterons ''attention'' alors que si l'on nous confie de tout surveiller avec attention, nous serons ''vigilants''.

Parmi les signaux faibles que perçoivent attention et vigilance, nous distinguons deux grandes classes :

- Les **anomalies** qui sont des écarts à la référence et qui présentent trois modes de référence principaux que sont: la **familiarité** « *on passe toujours là, quand c'est comme ça c'est normal* » ;
- l'***habitude*** ;
- et, le ***prescrit*** « *c'est comme ca* ».

Ce qui fait réagir c'est la non conformité à la référence ou le fait de ne pas être comme cela devrait être.
Les **précurseurs**, pour lesquels on connait déjà le lien de causalité *(je vois la fumée → il y a peut-être un feu)*. Le précurseur est un signal faible qui permet d'alerter, de donner du sens.



La gestion des signaux faibles présentée ci-avant présente quatre barrières successives :

- La 1ère barrière est celle de la reconnaissance *(a-t-on vu le signal ?) ;*
- La 2ème, elle de la pertinence *(signal suffisamment pertinent pour être traité ?) ;*
- La 3ème, principale, celle du niveau d'énergie face au signal *(est ce suffisamment grave pour le transmettre ?) ;*
- La 4ème, enfin, celle de la priorité donnée au signal par rapport aux autres sollicitations à traiter.

Quand le signal a franchi ces 4 barrières, il peut y avoir action pertinente permettant d'éviter la catastrophe.
Il faut également distinguer ''l'**urgence**'' de ''la **crise**''. L'urgence concerne des situations dangereuses, mais prévues alors que la crise naît au moment ou l'organisation est déstabilisée. Plusieurs facteurs peuvent déclencher la crise. Quand deux ou plus de ces facteurs sont concurremment présents on rentre véritablement en crise :

- Le facteur ''**surprise ou rapidité**'' ; si l'organisation n'est pas prête elle sera vite débordée ;
- Le facteur ''**étendue du sinistre**'' dans l'espace et en nombre de victimes ;
- Le facteur ''**rupture de communication**'' ; on ne sait à qui parler ni comment entrer en liaison ;
- Le facteur ''**incertitude''** ; les avis divergent et diffèrent sur la gravité … ;
- Les facteurs ''**cascade des évènements**'' et ''**insuffisance des ressources**''.

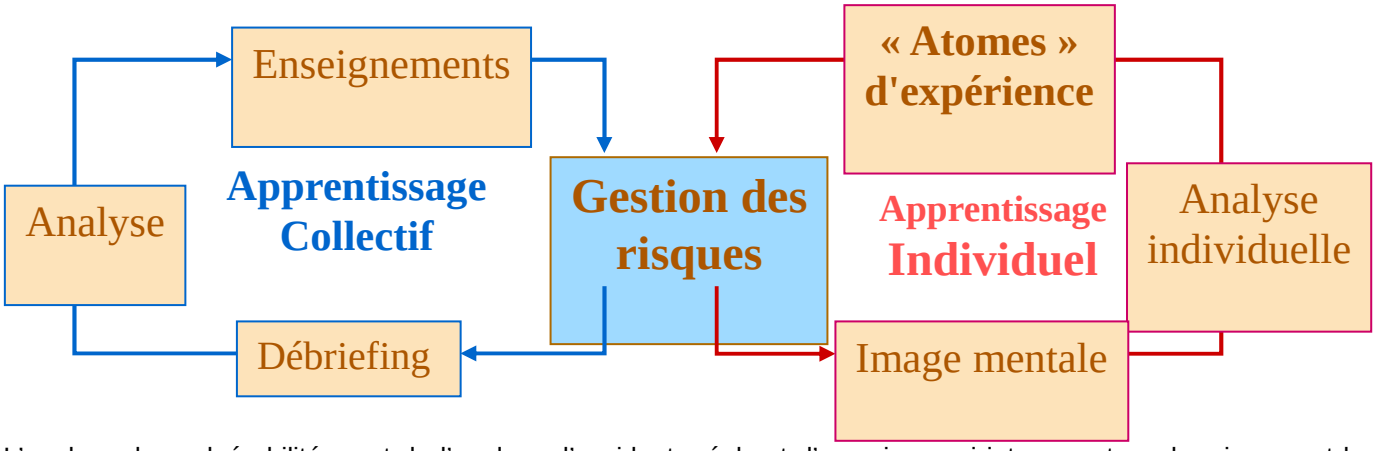
Pour anticiper et prévenir le basculement en crise, il faut ''baliser'' dans quatre directions :

- le **contrôle** : quels processus concernés ? Quelles incertitudes ? Quelles possibilités d'observation ? … ;
- l'**organisation** : existe-t-il un plan adapté ? Quel niveau de confiance et de respect au sein de l'entreprise ?
- le **sens** : tous les acteurs ont ils les mêmes données à jour, la même interprétation ?
- les **moyens** …

La construction collective de sens est l'un des points clés de réussite car une vision collective est indispensable à une coopération efficace. La **percolation** est également un sujet important : tous les nœuds du réseau d'acteurs ont-ils reçu l'information ? L'information est elle toujours valide ?

Trois facteurs sont à regarder :

- **l'exhaustivité** des récepteurs d'information ? **A qui** transmettre l'information et **à quel moment** ? ;
- **Combien de temps** l'information reste valide ? Attention ! La percolation cesse dès que certains acteurs ne reçoivent plus la même information ;
- **Apprentissage** et le **retour d'expérience** - REX - sont également essentiels. A partir du REX on évalue les vulnérabilités en se basant sur les menaces, les enjeux et les capacités d'actions.



L'analyse des vulnérabilités part de l'analyse d'accidents réels et d'exercices qui interrogent sur les risques et leurs formes, sur la nature des enjeux vulnérables, la population, l'environnement, l'économie. L'enjeu le plus important est de plus en plus souvent celui de l'**image mal gérée.**

Conclusion.
La maitrise des risques et la prévention des crises constituent une boucle de progrès qui impose d'anticiper, d'évaluer les menaces et les vulnérabilités, d'organiser la vigilance et l'attention, d'être en mesure de gérer la situation pendant qu'elle évolue, de savoir communiquer, de construire du sens à partir des retours d'expérience et de s'adapter sans oublier de valoriser ceux qui ont eu un comportement positif durant les situations d'urgence et de crise.

Exposé de M. Eric Wiatrowski

Chief Information Security Officer (CISO) - Orange Business Services

Orange Business Services, OBS est représentée dans 220 pays et emploie, 20 000 des 170 000 collaborateurs du groupe. Elle reçoit les politiques de continuité d'activité du Groupe et les décline dans ses divisions. La politique de continuité d'activité d'OBS fait l'objet d'un document de référence de quatorze pages qui définit les grands principes actés : raison de la continuité d'activité, problématique d'image, profitabilité, confiance des clients. Y figure également le comment : quelle mise en œuvre, quels ''steering comittee'', quelle protection pour les employés, quelle continuité pour les clients ? Politique visée par le Directeur Exécutif de OBS.

Les sites OBS assurent soit du support aux clients, soit de la production. Quelques-uns ont également en charge la supervision de réseaux ou de sécurité et bénéficient à ce titre d'une continuité d'activité en cas de sinistre majeur. Toute activité est doublée et chacune d'elle est backupée hors site. La continuité s'appréhende d'abord au niveau local mais cela ne suffit pas. On pense alors à la continuité d'activité globale. La réflexion a été menée par le Groupe puis a continué par OBS au travers de « sponsors », membres du COMEX, attentifs aux signaux faibles. Au niveau organisationnel, les centres opérationnels appliquent les process qualité up to date et les ''meilleures pratiques'' ITIL.
Rappelons que les fondamentaux de la continuité sont de protéger le personnel, préserver les biens et maintenir au meilleur niveau les activités opérationnelles pour protéger l'image de marque et conserver les parts de marché.
Gérer la crise, c'est manager l'improbable avec flexibilité. Les collaborateurs et les clients doivent pouvoir prendre des décisions éprouvées sachant qu'au-delà des process, chacun dispose de son libre arbitre pour prendre une décision pertinente basée sur son expérience. La communication doit être interne et externe.
Eric WIATROWSKI rappelle les évènements dramatiques du Caire en janvier 2011. Les clients gérés par le Caire le matin étaient reportés sur l'Inde et la zone Amérique l'après-midi. Au bout de quelques jours, il fut décidé de passer en mode secours qui avait été testé sur le papier mais jamais sur une telle échelle et en temps de crise. Il y eut des transferts de responsabilité entre les trois sites et tout s'est passé efficacement par échange de mails et autres services de communications entre Egypte, Inde et Amérique du Sud. Par la suite, IDC réalisa une analyse notamment

sur la gestion de la crise, analyse concluant qu'en intégrant en plus le site de Maurice, il serait encore bien facile de gérer la crise, notamment sur la plaque Europe.

Comment bâtir la boucle d'amélioration ? On utilise les grands principes BS 25299 et la version ISO 23001. Le REX RETEX permet de tirer des enseignements de ce qui se passe en période de tests ainsi qu'en situation réelle. Enfin, s'agissant de la prise de décision, retenez que lorsque vous basculez un centre de 1 000 personnes qui supporte de très nombreux clients, la décision réelle est difficile à prendre…

Débat

Intervenant : Vous parlez de la gestion de crise mais le client dans tout ça ? Quand est-il de la communication vers l'extérieur ?

E. WIATROWSKI : La cellule communication est souvent « frileuse » car il est nécessaire de trouver le point d'équilibre entre trop en dire ce qui risque de se retourner contre l'entreprise et pas assez. Cette cellule hésite souvent à faire une diffusion générale, médiatique et répond plutôt aux questions posées. On est plutôt dans un mode réactif qu'actif mais cela risque d'évoluer avec les nouvelles obligations qui demandent de prévenir les personnes lorsqu'elles sont susceptibles d'avoir été hackées. Il faudra alors être plus proactif.
J.L WYBO : La communication au travers des réseaux sociaux, Twitter notamment, est un nouveau facteur à prendre en considération. On observe une espèce de frilosité. Vous pouvez avoir des dizaines de petits messages non formalisés qui décrivent la situation en cours alors que l'équipe de communication réfléchit encore au communiqué qui va être publié !
De grandes entreprises ont maintenant des cellules Twitter qui font de la veille permanente et leur permet d'avoir une réactivité immédiate. Il faut dans ce cas être dans « le proactif » mais il faut faire très attention au « parler vrai ». Dire que l'on ne sait pas et que l'on cherche plutôt que l'on sait et s'apercevoir après que l'on ne savait pas peut nuire sérieusement à l'image de l'entreprise.
Le Virtual Support Operation Team (VOST) est nouvelle forme de communication. Cette équipe formée de personnes qui ont une compétence spécifique dans les réseaux sociaux va surveiller ce qui se dit et lorsqu'il y a un problème qui concerne l'entreprise, ces personnes vont s'activer et seront chargées de répondre sur les réseaux sociaux à partir des éléments de langage qu'on leur donne, ce qui permet à l'entreprise d'avoir une grande réactivité. Mais attention avec ce genre de communication, car une entreprise qui crée un compte Twitter doit être capable d'interagir car vous pouvez être vite débordé et l'image de l'entreprise en pâtira.
Enfin, Il est très important de définir qui est autorisé à parler ou à donner les éléments de langage (factuels) au sein de l'entreprise.

Int. : Lors de la crise du Caire, combien de temps avez mis avant de passer en mode de repli et qui a pris la décision au final ?
E. WIATROWSKI : Les évènements ont commencés le 25 janvier, on a compris que le 28 cela allait mal et le 1er février c'était basculé. La décision a été prise de façon consensuelle, c'est plutôt au niveau de l'état major.
J.P WYBO : Lors du séisme en Haïti, la filiale de Total qui fournit de l'essence, du gaz et du fioul, s'est retrouvée avec un bâtiment abimé et a dû évacuer. La bascule s'est faite en une heure maximum et cela a été un franc succès. Trois jours après ils avaient restauré 100% du business. La décision a été prise collectivement par les 2 patrons du site d'Haïti, le bureau régional qui se trouve à Panama et le siège à Paris. La communication vers Haïti a été coupée sauf pour le PC régional qui est à Panama (même fuseau horaire). Des points tactiques étaient faits 2 fois par jour et ensuite Panama faisait des points stratégiques avec Paris une fois par jour et une fois par jour, ils envoyaient un mail à toutes les personnes concernées du Groupe afin que tout le monde ait la même information.

Int. : Vous n'avez pas parlé des cellules d'experts et la manière dont elles doivent être pilotées.
J.P WYBO : La grosse difficulté de faire coopérer des gestionnaires de crise et des experts c'est d'arriver à trouver une représentation commune de ce qui se passe . Par exemple dans une cellule de crise préfectorale, on étudie des exercices qui donnent lieu à un nuage toxique (chimique ou radiologique). Vous avez l'expertise du nuage toxique, la propagation du nuage avec les modèles très sophistiqués capables de voir comment le nuage va passer dans les immeubles, à l'intérieur des appartements …. Vous avez ces données avec les résultats de simulation, vous avez l'expert et vous avez les décideurs et d'un exercice à l'autre cela n'a rien à voir. Vous avez des décideurs qui vont demander des données et des avis à l'expert et d'autres fois l'expert ne sera pas sollicité.
Ce qui est très important, c'est de bien comprendre qu'un expert ne fait pas d'aide à la décision mais il fait de l'aide à la compréhension de la situation car on n'aide pas un décideur à décider.
Le décideur doit prendre en compte non seulement l'expertise technique mais aussi le social, l'entreprise, les relations, les clients, les médias et c'est l'ensemble de cela qui fait qu'il prend une décision qui n'est peut être pas la

meilleur techniquement mais qui est peut être celle qui n'est pas irréversible ou qui est la plus consensuelle en terme de résultats. Accepter tout ce que les experts disent, cela revient à déléguer sa décision.
L'expert doit juste apporter des éléments de clarification et le décideur prendre des décisions.

Présentation des orateurs

Jean-Luc WYBO
Ingénieur de l'INSA de Lyon, docteur en informatique et HDR en gestion des risques. Maître de Recherches au CRC (Centre de recherche sur les Risques et les Crises) de Mines ParisTech et professeur invité à l'université de Tongji (Shanghai, Chine). Rédacteur en chef de la revue *Safety Science* (Elsevier) et de *l'International Journal of Emergency Management* (Inderscience). Membre des Conseils Scientifiques du CSFRS, de l'ENSP et du comité de pilotage scientifique du Défi « Liberté et sécurité de l'Europe » de l'ANR. Auteur du livre « Maîtrise des risques et prévention des crises » chez Lavoisier.

Eric WIATROWSKI
Chief Information Security Officer (CISO) d'Orange Business Services depuis 2001.
Il a travaillé au CERN, à l'Université, et cumul 30 années d'expérience dans les Télécommunication sur les normes, le développement de services Internet, et leur marketing en France et à l'international. Acteur des certifications ISO 15408 et ISO 27001. Ingénieur Supélec, certifié ISMS Risk Manager, il est reconnu Orange Security Expert.