Activités d'Importance Vitale

De l'analyse au management des risques

Cyril Mourlon[1]

[1]THALES D3S, Consulting, Immeuble le Phénicien, 24-26 quai Alphonse le Gallo 92100 Boulogne-Billancourt

cyril.mourlon@thalesgroup.com

Résumé –Nous allons nous attacher dans cet article à traiter de la meilleure approche pour anticiper, réagir, traiter un risque pouvant atteindre une activité vitale. Cela ne peut s'improviser et notre conviction est les entreprises puissent disposer d'une méthode adéquate pour la meilleure perception du risque lié à une activité vitale et pour la meilleure préparation face à ce risque potentiel.

Abstract – *This article wishes offer an overview of the best approach to anticipate, react, manage a risk which could occur against a critical business. We are convinced that firms can have an appropriate method for the best perception of the risk linked to a critical business and for the best preparation for this potential risk.*

1.Introduction

La vie économique des entreprises traverse des situations multiples alternant les périodes de croissance et les périodes de rigueur. Face à l'imprévu, l'entreprise développe sa propre capacité de résistance et de réaction, et dans le meilleur des cas dispose d'une stratégie de défense face aux risques qui pourraient réduire de manière significative ses activités essentielles.

Or les entreprise doivent s'adapter à des contextes de plus en plus difficiles. Cette adaptation, liée à la capacité de réflexion, d'appréhension et de perception d'une situation nouvelle, se traduit pour une entreprise par sa capacité à s'organiser adroitement et adéquatement, notamment face à des événements graves et souvent nouveaux. A titre illustratif, les développements technologiques, permettant une plus grande efficacité et d'un plus grand confort dans les processus des entreprises, cultivent également de menaces telles que les virus, la cybercriminalité, le cyberterrorisme, etc..

La question se pose donc, de savoir comment pour une entreprise et a fortiori une entreprise ou une organisation concourant une activité d'importance vitale doit-elle s'y prendre pour prévenir et protéger ses infrastructures essentielles contre les nouvelles menaces d'aujourd'hui et de demain ?

2.Les secteurs d'activités d'importance vitale

Depuis le début du millénaire, l'Etat français a mûri une réflexion permettant de passer d'un point sensible à un point d'importance vitale appartenant à un Secteur d'Activités d'Importance Vitale. Cette réflexion a pu aboutir à la modification du code de la Défense (articles L. 1332-1 à L. 1332-7) par la loi n° 2005-1550 du 12 décembre 2005 , suivi du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale, et de quelques arrêtés.

Ce nouveau cadre réglementaire introduit une notion intéressante de partage de responsabilité entre les opérateurs concourant à maintenir une activité vitale. Plus précisément, *les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel industriel militaire ou économique, la sécurité ou la capacité de survie de la Nation, ou dont la destruction ou la détérioration pourrait présenter un danger grave pour la population, sont tenus de coopérer, à leur frais, à la protection de leurs établissements, installations ou ouvrages contre toute menace, notamment à caractère terroriste*.

La loi apporte également un élément profitable en précisant la démarche à suivre. Il s'agit de conduire une analyse de risque permettant d'identifier et de définir les scénarios contre lesquels le secteur, et a fortiori les opérateurs, doit absolument se prémunir.

Toutefois, même s'il est recommandable, l'exercice n'en est pas moins difficile : Quel doit être le niveau de profondeur ? Quelles sont les attentes des acteurs concernés ? Comment disposer de résultats pertinents ? Peut-on réellement déterminer que telle activité pourra ou ne pourra pas absorber un événement tel un typhon, un séisme, un multi-attentats ou encore une crise sanitaire nationale ?

Les réponses à ces questions montrent que le sujet dépasse le seul domaine de la sécurité ou de la sûreté car il engage toute l'activité dans son ensemble des entreprises concernées.

3.La gestion des risques

La gestion des risques dans les entreprises se fait au quotidien par des compétences très circonscrites. Au plus haut niveau des organisations, le risque financier et stratégique est adressé le plus souvent par la direction générale. L'hygiène, l'environnement, les opérations de production, la gestion de projets, le patrimoine immobilier, le système d'information sera traité par des experts et de responsables, autonomes dans leur domaine. Toutefois l'interrogation est entière quant à réussir à créer des liens effectifs et transversaux entre les domaines.

Quand une entreprise perçoit un risque majeur, elle peut décider d'optimiser ses coûts de couverture selon quatre possibilité :

- ne rien faire ;
- éviter que l'événement arrive ;
- transférer sur un « tiers risqueur » ;
- réduire en couvrant adéquatement le risque au travers d'un investissement pondéré au gain quantitatif et qualitatif estimé.

Dans ce dernier cas, l'entreprise doit examiner ses capacités de transformation pour renforcer sa permanence tout en garantissant sa performance en situation difficile. Dans ce type de réflexion, la notion de permanence est une réalité à rapprocher de celle de la performance. Quel que soit l'événement perturbateur, l'activité doit être de qualité, fournie à temps, aux plus près des clients ou des usagers. Les coûts d'investissements doivent être optimaux sous maîtrise des directions opérationnelles et financières.

Des risques majeurs, même s'ils semblent parfois peu crédibles ou impossibles, peuvent porter durablement atteinte aux activités critiques d'une entreprise : explosion de site, perte de personnel clé dans un accident collectif (avion, train,…), malveillance interne… Les menaces asymétriques, définies comme une disproportion entre les moyens utilisés et les impacts subis sont également à considérer : la vengeance d'un employé contre son employeur en supprimant des informations servant aux bons fonctionnements des processus clés de l'entreprise, la communication aisée d'informations stratégiques et concurrentielles par des employés autorisés, l'atteinte à l'image de l'entreprise ou à la réputation des décideurs via les médias, etc…

Pour la majorité des organisations, la réponse à une menace identifiée est bien souvent une réponse financière et technique, dont les solutions doivent être déployées rapidement. Une entreprise subissant des intrusions répétées dans ses bâtiments, va très certainement investir rapidement dans un contrôle d'accès ou dans un gardiennage, sans pour tant procéder à l'analyse qui lui permettrait de savoir ce qui la rend si « attractive » et si les solutions sont adéquates en terme de couverture du risque considéré.

Trois points doivent être considérés :

- les enjeux de l'entreprise sont en général mal perçus et quand s'il sont perçus correctement, ils sont souvent mal partagés par l'ensemble des employés ;
- les besoins de protection des activités vitales ou critiques sont rarement correctement exprimés ;
- les impacts redoutés ne sont pas ou peu définis, discutés et partagés au sein de l'entreprise et des personnels concernés.

Face à ce constat, les entreprises et les organisations doivent développer une responsabilité et un engagement approprié par rapport à leur activité et à l'ensemble des risques sous-jacents au travers d'une méthode adéquate.

Il est envisageable de proposer une méthode d'analyse rationnelle, non partisane, intégrant les besoins de performance des entreprises ainsi que les aléas propres au contexte d'évolution. Cette méthode doit être déployée, utilisée, recherchant une fédération des décideurs sur ce que l'entreprise est prête à subir ou, au contraire, ce qu'elle ne veut ou ne peut absolument pas supporter.

4.Une méthode en quatre étapes

Il s'agit donc de donner à une entreprise ou à un opérateur d'activité d'importance vital un outillage et un référentiel efficient pour analyser, anticiper, coordonner son action en vue de minimiser ses pertes humaines, financières ou encore liées à sa connaissance et à son savoir-faire en cas de risque avéré.

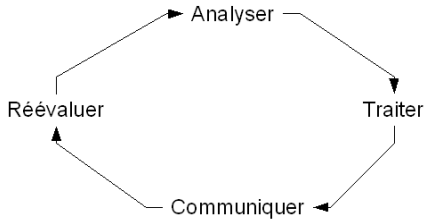

FIG. 1 : la gestion des risques

4.1De l'importance d'analyser

Des analyses systémiques doivent pouvoir être menées. Il s'agit d'analyses qui cherchent à définir exhaustivement et le plus adéquatement possible les objectifs de prévention et de protection à atteindre et traduits eux-mêmes en termes de performance.

Peu de méthodes topiques semblent exister pour analyser globalement l'ensemble des risques d'une activité vitale.

La méthodologie EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) pourrait être une des plus adaptées pour ce type d'analyse de part sa démarche en 5 étapes :

- **étape 1 :** Étude du contexte et notamment, celui du secteur d'activité d'importance vitale ou plus précisément, celui de l'opérateur d'infrastructure vitale concerné ;
- **étape 2 :** Expression des besoins de protection, contribuant à l'appréciation des risques, en formalisant les impacts inadmissibles (danger pour la population, atteinte à l'exercice de l'autorité de l'Etat,...) ;
- **étape 3 :** Étude des scénarios de menaces, recensant et hiérarchisant les événements à analyser ;
- **étape 4 :** Identification des objectifs de sécurité, permettant de; après avoir formalisé et hiérarchisé les scénarios de risques, proposé des objectifs de protection des infrastructures vitales ;
- **étape 5 :** Détermination des mesures de sécurité en lien avec les plans de vigilance et de réaction gouvernementaux.

Ce type d'outil est néanmoins à adapter pour analyser n'importe quel risque sur n'importe quel secteur d'importance vital. Une adaptation nécessaire sera différente selon le contexte de l'opérateur concerné. Par exemple, l'expérience nous a montré sur un SAIV que l'analyse du contexte devait mettre en en lumière tous les processus critiques du secteur ainsi que tous les opérateurs concernés. L'analyse de la menace doit traiter, sur des grandes familles de menaces (terrorisme, pandémie, phénomène climatique d'ampleur) conjointement la malveillance avec des échelles de faisabilité appropriée et l'accidentel avec des échelles statistiques adéquates. Les objectifs doivent traiter à la fois la prévention de la menace et la protection en cas de risque avéré. Enfin, le nombre de scénario de risque doit être limité aux risques les plus critiques et surtout pouvant être traités par des mesures acceptables et réalistes pour l'organisation concernée.

L'analyse est néanmoins bénéfique. Elle permet une prise de conscience salutaire sur la fragilité d'une organisation concernant sa capacité à réagir et à se réorganiser en cas de tous les types de crise envisageables et surtout permet de préparer la meilleure décision en terme de traitement.

4.2De l'importance de traiter

La définition des rôles et responsabilités est une opération clé pour la réussite de ce type d'exercice. Il est important de distinguer plusieurs rôles :

- Celui qui va analyser la situation, les activités et qui va définir les risques majeurs pour les activités vitales ;
- Celui qui va décider la manière de traiter le risque ;
- Celui qui va approuver, par son autorité, la décision et qui va engager financièrement l'organisation à se protéger ;
- Celui qui va définir, choisir la solution et la déployer dans l'entreprise ;
- Celui qui va contrôler la performance de la solution.

4.3De l'importance de communiquer

Il est raisonnable de dire que le risque avéré induira une crise qui devra être gérée en partie par l'opérateur. Les experts s'attachent à dire que la gestion de crise repose sur 80% de la communication ciblée. La désorganisation probable de l'opérateur, le besoin de réaction et de reprise de la situation par celui-ci sera envisageable dès lors que les canaux de communication ne seront pas saturés. Pour cela, l'anticipation est essentielle. Les plans de communication doivent être formalisés, des exercices de simulation de crise ou de risque avéré doivent être conduits pour aider les personnels à se préparer à la réaction.

4.4De l'importance de réévaluer

Enfin le contrôle périodique de performance des solutions déployées doit amener un opérateur à mesurer sa capacité à réagir face à un risque selon le niveau de traitement prévu. Un opérateur d'infrastructure vitale, quelque soit son niveau d'agilité, devrait pouvoir s'adapter à la menace à tous les niveaux internes de son organisation. Pour cela, son référentiel de prévention et de protection doit être contrôlé au niveau de sa performance mais aussi de sa pertinence compte tenu de l'évolution des contextes et des environnements dans lesquels se trouvent les opérateurs.

5.Conclusion

La philosophie grecque induit que l'excellence est un art que l'on n'atteint que par l'exercice constant. Reprenant à notre compte cette proposition, nous pourrions conclure en présentant un management global des risques d'excellence en trois mouvements :

- **l'anticipation** au travers de toute la planification nécessaire à tout opérateur d'infrastructure d'importance vitale,
- **la coordination des forces et des acteurs** régissant un risque pouvant atteindre un service vital,
- **l'élévation du niveau de connaissance** en matière de gestion de risque.

La gestion des risques est un art qui demande un effort constant d'analyse, de traitement, de communication et de réévaluation. Pour porter l'analyse, les organisations ont besoin d'un outil tel que la méthodologie EBIOS, qui bien utilisée, permettra au gestionnaire des risques de l'entreprise, quel qu'il soit, de bâtir un référentiel spécifique, adéquate et utile à tous les acteurs et à toute l'organisation de l'opérateur vital et pourra proposer un management de risques unifié et cohérent au sein de son activité.