NEWSLETTER

dédiée à la gestion des risques dans le secteur public

PRIMO

IPGR

PÔLE RISQUES

MARSH

SOMMAIRE

LE MOT DU PRESIDENT

Chers collègues,

Dans cette nouvelle newsletter de Primo France, nous avons axé notre communication sur deux sujets : le Label de Gestion des Risques Territoriaux, et les cyber-risques.

Le Label, car il est un outil qui permettra, à moyen et long terme, d'inclure la notion de gestion des risques dans les systèmes de gouvernance des collectivités territoriales et de faire face aux nouveaux défis du secteur public en matière de prévention de ces risques, en formant les agents de tous les niveaux à prendre en compte ce facteur dans leurs décisions quotidiennes.

Le dossier spécial sur les cyber-risques permet quant à lui d'avoir une meilleure idée des dangers en ce domaine très spécifique du numérique, sur lequel l'humain compte de plus en plus. Les mises en garde sur les machines valent également pour leurs créateurs et leurs utilisateurs. Les experts interviewés ici recommandent une vigilance constante en la matière, et prodiguent quelques conseils qui seront utiles à tous.

J'en profite pour vous inviter ici à une conférence qui se tiendra le 2 Juillet à Lyon, sur ces deux sujets. Veuillez voir le programme détaillé ici.

Je vous souhaite une bonne lecture et vous invite également à naviguer sur le site PRIMO France pour de plus amples informations.

Gérard COMBE

Président de Primo France

<u>FOCUS</u> : Le Label de Gestion des Risques Territoriaux et les assureurs
Comment le Label GRT peut-il jouer dans la tarification des primes d'assurance?

Appel d'offres infructueux, hausse des primes ou encore résiliation unilatérale de contrats, les relations entre collectivités et assureurs ont connu ces dernières années quelques tensions. Il n'en a pourtant pas toujours été ainsi et le marché est en phase d'attirer de nouveau la convoitise des acteurs du secteur. En effet, s'il est reproché au marché public son manque de flexibilité et son formalisme administratif, la prise de distance des assureurs s'explique en partie en raison d'un fort taux de sinistralité et d'une appréhension face à des risques souvent mal recensés.

Or les collectivités ont compris la nécessité d'évaluer et de gérer leurs risques. Leur maîtrise devient un enjeu stratégique au sein du secteur public et on constate une montée en puissance des collectivités sur ce sujet. Certaines collectivités sont déjà dotées de directeurs de gestions des risques, lesquels s'arment contre la survenance des risques en effectuant des audits et des mises à jour régulières. Mais il ne s'agit encore que d'une minorité. Cette pratique en est encore à ses balbutiements.

Pourquoi les collectivités territoriales intéressent les assureurs ?

Les collectivités territoriales présentent des risques variés, polymorphes, qui requièrent une réactivité croissante de la part des élus et de leurs équipes.
Aussi de plus en plus de collectivités ont des risques managers qui s'arment contre la survenance des risques en effectuant des audits et des mises à jour régulières. Ils sont également chargés de la prévention, faisant de la maîtrise des risques un sujet stratégique au sein du secteur public.
(cf. l'article sur ce sujet ici)

Quelles sont plus-values du Label GRT?

Le référentiel du label a été construit en suivant les principes et les lignes directrices de la nouvelle norme mondiale ISO 31 000 sur le management des risques. Il permet ainsi à la collectivité des bénéfices organisationnels, économiques et juridiques.
Le Label permet :
- d'accompagner les collectivités dans la réduction de leurs vulnérabilités et de développer une gestion opérationnelle plus optimale,
- de donner un cadre solide aux responsables avec un outil d'aide à l'amélioration continue,
- d'attester d'une bonne gestion et de l'implication de la collectivité auprès de ses administrés et de ses partenaires.

Ce label accroît la visibilité de l'investissement des collectivités en matière de Risk Management.

Quels travaux ont été réalisés jusqu'ici ?

Des rencontres avec plusieurs assureurs ont permis de tirer les conclusions suivantes sur le marché.
Les collectivités territoriales présentent des profils de risques complexes, et les démarches de passation des marchés publics d'assurance se révèlent contraignantes et exigeantes ; de plus, le marché souffre d'un manque d'ajustement de l'offre et de la demande, ce qui génère peu de concurrence lors des consultations.
De plus, les assureurs déplorent un manque d'informations et une culture de la gestion des risques réduite à son strict minimum. Ce manque de précision rend difficile la réponse à un appel d'offre.

Quelles sont les prochaines étapes ?

Le but du Label est de combler toutes ces lacunes, afin que les collectivités puissent négocier sur des bases saines, grâce à une méthode simple : les notes reçues lors des entretiens de labellisation seraient pondérées, afin de créer une note « Assurances », laquelle serait la base pour une simplification des polices de Responsabilité Civile et Dommages. Parmi les préconisations données aux collectivités labellisées, une aide sera apportée à la bonne structuration d'un cahier des charges optimal.

Nous sommes donc actuellement dans une phase de transition. L'implication des élus et l'appui de soutiens reconnus tels que Marsh ou Primo permettront d'accompagner les collectivités dans cette démarche.

Le Label GRT peut fournir une impulsion. Le lancement d'un appel d'offres demande une parfaite connaissance et une bonne maîtrise de ses risques. La mauvaise rédaction d'un cahier des charges poussent les assureurs à ne pas répondre ou bien à hausser les primes et les franchises par précaution. A contrario, un inventaire exhaustif des risques à assurer, la mise en avant des actions de prévention et la capacité à définir ses besoins d'assurances permettront aux assureurs d'élaborer au mieux leur proposition et d'assurer ainsi une meilleure protection et une optimisation des coûts.

Interview de M. Yves Le Floch,
Directeur du Développement de la Cybersécurité chez SOGETI.

(Extraits)

Sogeti (**So**ciété pour la **G**estion de l'**E**ntreprise et **T**raitement de l'**I**nformation) est l'un des leaders des services informatiques et d'ingénierie de proximité ; elle est également partenaire de Marsh France pour la maîtrise et le transfert des cyber-risques.

1/ A quels cyber risques les collectivités locales et autres entités publiques peuvent-elles avoir à faire ?

La cybersécurité sert principalement à protéger trois aspects du système d'information : la confidentialité, l'intégrité et la disponibilité des données.

Ces données peuvent être attaquées par trois types d'agresseurs, qui ont leurs propres motifs et des capacités techniques de plus en plus avancées.

Le premier type de cyber-agresseur sera le délinquant, qui volera les données pour les revendre au plus offrant. Ou encore utilisera un « ransomware » ou « rançongiciel » : ce logiciel malveillant permet de chiffrer les dossiers, de prendre en otage les données et parfois de bloquer l'accès à un réseau ; les propriétaires doivent alors payer la rançon pour récupérer leurs données, sans jamais être certains de leur récupération correcte, ni du fait que le tout n'ait pas été revendu.

On peut aussi avoir affaire à une cyber-agression d'ordre idéologique, telle que le vol de données confidentielles ou privées à des fins de publication en ligne, pour ainsi ternir l'image de la personnalité ou de l'organisme visé. Un autre type d'agression est la défiguration d'un site web, celui d'une mairie par exemple, en changeant des photos ou insérant des messages politiques. De nombreuses collectivités territoriales sont chaque année victimes de tels agissements.

Les deux premiers agresseurs ont aussi un mode d'attaque en commun, qui est de saturer les sites visés, provoquant ainsi un sabotage nommé « attaque en déni de service » qui empêche tout accès au site.

Il existe aussi des agresseurs d'ordre stratégique, souvent très sophistiqués, qui sont eux liés à des Etats et récupéreront des données technologiques, opérationnelles ou stratégiques à des fins d'espionnage.

[…]

3/ De plus en plus de mairies et d'agences de l'Etat offrent des services numérisés, comme des demandes en ligne de documents administratifs. Quels sont vos conseils pour éviter l'usurpation d'identité ou le piratage des données ?

Le problème en France est qu'il n'y a pas de système d'authentification à distance fiable, car les politiques ont toujours reculé sur la création d'une carte d'identité à puce utilisable pour prouver son identité via internet. Ainsi, lors d'une demande administrative en ligne, il n'y a aucun moyen sûr de savoir si le demandeur n'est pas un imposteur, car n'importe qui peut se faire passer pour moi.

Il n'y a pas de solution vraiment sûre pour régler cette question de l'authentification, il faut donc se contenter de systèmes existant. Pour une demande d'état civil, par exemple, aucune preuve d'identité n'est demandée ; pour l'accès au dossier fiscal, Bercy se contente d'identifiants transmis par courrier ; pour des échanges vraiment sensibles, l'administration française doit trouver d'autres solutions.

Un moyen simple est d'ouvrir un compte personnel en mairie, après justification de son identité, avec attribution d'un mot de passe personnel. Le mot de passe est loin d'être un moyen sûr, mais c'est déjà un début d'authentification. Et dans tous les cas, le chiffrement des données est un impératif, dès lors qu'il s'agit de données sensibles ou personnelles, aussi bien lors des échanges que lors du stockage.

Mais je vais surtout insister sur un point particulier : les collectivités territoriales, et les entités publiques en général sont tenues par la loi d'appliquer le Référentiel Général de Sécurité, notamment pour les téléservices. Le RGS est un document technique, qui explique les démarches professionnelles à effectuer, comme l'analyse des risques auxquels on est exposé. Il est important de le respecter et de le faire respecter, y compris lorsque l'on confie certains services ou développements informatiques à une entreprise prestataire.

Voir l'article complet ici.

Pour en savoir plus sur SOGETI, et son partenariat avec l'UGAP, cliquez sur les liens suivants :
http://www.fr.sogeti.com/node/671
http://www.ugap.fr/
http://www.fr.sogeti.com/

Pour en savoir plus sur le RGS et la CNIL, cliquez sur les liens suivants :
http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/
http://www.cnil.fr/

Le Mot du Courtier sur les cyber-risques

M. Luc Vignancour, Directeur Adjoint Risques Spéciaux chez Marsh France, répond à nos questions.

Primo : Concrètement, que fait l'assureur ? Quelle différence avec ce que nous a dit M. Le Floch ?

Luc Vignancour : C'est très simple.
M. Le Floch parle de tout ce qu'une entreprise ou une entité publique peut ou doit faire face au risque, afin de réduire sa probabilité et son impact.
Mais on ne peut supprimer entièrement ce risque, bien entendu. Toutes les personnes en charge de la cyber - sécurité le savent, le risque « zéro » n'existe pas.
Une fois que le risque est survenu, ce qui arrive, l'entité publique, ou l'entreprise, a alors besoin de mettre en route un protocole de gestion de crise.
Ce protocole coûte bien sûr de l'argent, et ce coût peut s'ajouter à d'autres pertes encourues lors de la cyber – attaque : réclamations de tiers, pertes commerciales ou autres.
L'assurance va prendre en charge ces coûts-là. Celui de la gestion de crise, celui des pertes, etc.
Il est donc nécessaire de connaître la couverture prévue lorsque ce risque arrive, et agir en fonction.

Primo : Quels autres services l'assureur offre-t-il ?

Luc Vignancour : L'assureur peut, en plus de la prise en charge standard des pertes et surcoûts, proposer des services de notification et de gestion.
Pour la notification, il s'agit de faire remonter la déclaration de l'attaque aux autorités compétentes, et ainsi de s'occuper administrativement des suites du risque.
Quant à la gestion, il s'agit de celle de la crise, dont l'assurance peut s'occuper en lieu et place de l'entité attaquée.

Primo : Le mot de la fin ?
Luc Vignancour : Assurez-vous ! De préférence, chez nous !

ACTUALITE DE NOS PARTENAIRES :

Notre partenaire Marsh a été représenté au **Forum Dii** (Development Institute International) à l'occasion du 13e Forum Annuel, sur le thème « Les nouveaux Partenariats Public-Privé » (voir le site de l'évènement).
Le Forum s'est tenu **les 11 et 12 Juin à Paris**, et M. Thomas Graiff est intervenu le Jeudi 12 Juin, n'hésitez pas à consulter le programme sur le site.
A cette occasion, Marsh est intervenu sur les risques à prévoir et gérer lors des différentes phases de la mise en place d'un projet d'infrastructure : consultation, construction, exploitation.
Cet évènement a été l'occasion pour les entités publiques de mieux comprendre les mécanismes de transfert et de partage des risques entre le public et le privé, et de rencontrer les différents acteurs impliqués dans les projets d'infrastructure.

ACTUALITE DE PRIMO :

De son côté PRIMO France n'est pas en reste, **puisque comme le souligne le Président dans son édito se tiendra le Mercredi 2 Juillet une conférence au CESER de Lyon**, sur les cyber-risques et sur le Label GRT.
Voir le programme détaillé ici.