Jean-Laurent Santoni

Du risque informatique au risque informationnel

Juriste, courtier en assurance et surtout conseil en gestion des risques immatériels, Jean-Laurent Santoni pratique un métier d'interface à équidistance entre les assureurs et les clients. Il raisonne davantage en termes de problématiques que de solutions, dans une démarche plus globale de gouvernance, incluant la prévention, la protection et le financement du risque par l'assurance. Avec l'internet, le risque n'est plus seulement physique et matériel, il est immatériel et mondial. Mise au point sur ces mutations et les réponses possibles.

Sylvie Rozenfeld : Courtier en assurance, vous avez été consultant senior risques et assurances des systèmes d'information au sein de la filiale Conseil de Marsh, puis directeur de Marsh Risk Consulting France, avant de rejoindre Sageris, la filiale conseil et prévention de Gras Savoye, spécialiste du conseil en gestion des risques. Votre métier, c'est donc la gestion du risque immatériel.

Jean-Laurent Santoni : Je suis juriste de formation et mon premier métier, après un doctorat de droit des affaires, était conseil juridique et fiscal. Le conseil a donc toujours été ma ligne directrice. L'objet sur lequel je travaille porte sur les systèmes d'information, dans leur dimension informatique mais aussi informationnelle. Je dirais que je suis conseil en gestion des risques, l'assurance représentant la solution de financement du risque. L'assurance est généralement une solution pré-déterminée, que l'on pourrait présenter comme « disponible sur étagère ». Au contraire, je vais plutôt chercher le contrat de telle ou telle compagnie d'assurance, l'adapter et l'appliquer à mon cas particulier. Je cherche à éviter de reporter au moment du sinistre la question de savoir si le contrat était ou non bien adapté. Mon métier consiste donc à intervenir en amont, en raisonnant davantage en termes de problématiques que de solutions. Cela correspond à l'évolution actuelle sur la gouvernance des risques, la conformité, ce que les Américains appellent l'Enterprise Risk Management et qui se traduit en France par la reconnaissance du principe de précaution. Les risques sont acceptables et acceptés à condition d'être maîtrisés, quantifiés et connus.

« Nous avons donc une infrastructure éclatée avec des risques multiformes alors que la réponse en assurance reste encore très traditionnelle, avec des offres « sur étagère » qui couvrent l'informatique, pas nécessairement l'information. »

La vraie difficulté consiste à bien comprendre les évolutions et à éclairer le jeu de chacun. J'essaie d'avoir à la fois un pied du côté des assureurs pour étudier leur politique commerciale, leur capacité et leur envie de développer de nouveaux domaines et leur apporter mon savoir-faire et ma connaissance des risques ; et d'avoir l'autre pied dans le juridique, dans la technique et la gestion des risques des différents secteurs des clients. Je pratique un métier d'interface pour lequel je dois être à équidistance entre les assureurs et les clients afin de faire comprendre les problématiques des clients aux assureurs en termes de besoins de garantie et faire comprendre aux clients qu'un assureur ne va pas garantir n'importe quoi et que le financement du risque s'inscrit dans une démarche plus globale.

La prévention se trouve donc au centre de la gouvernance des risques informationnels.

Il y a bien sûr la dimension prévention, qui implique de faire en sorte qu'un sinistre n'arrive pas, mais aussi celle de la protection. Si l'événement survient, comment le gérer, comment y répondre, comment mettre en place une gestion de crise, comment indemniser. Le financement est la troisième dimension. Le risque étant accepté, la contrepartie de l'acceptation est qu'il y a une indemnisation. C'est le principe du risk management.

Pour revenir à la prévention, il faut identifier la probabilité d'occurrence d'un sinistre, identifier ce qui peut survenir, prendre des mesures préventives pour que cela n'arrive pas. Et quand l'événement survient, il faut analyser l'intensité du sinistre et se protéger de la force de son impact. La protection va intervenir pour réduire cet impact et pour le financer. L'assurance est une mesure de financement du risque. Avoir une assurance n'empêche pas d'avoir un sinistre. En revanche, une assurance limite l'impact d'un sinistre.

Concrètement, êtes-vous courtier en assurance ?

Quand je suis dans le rôle de courtier, cela veut dire que je termine mon travail (sauf la survenance du sinistre, où je suis bien sûr présent). Je suis arrivé au bout d'un cycle qui consiste à analyser le risque, à comprendre les probabilités d'occurrence d'un sinistre et à en mesurer les impacts. A partir de cette analyse, je cherche sur le marché des polices d'assurance qui correspondent à la situation. Ces réponses peuvent être contractuelles, mais également techniques. Par exemple en matière de failles de sécurité, il convient de mettre en place des mesures de notification de la faille de sécurité à la Cnil et à tous ceux qui l'ont subie. Dans l'affaire Sony, la divulgation des données personnelles avait concerné des millions de personnes. Nous sommes désormais dans l'assurance service. Nous ne sommes plus dans l'intermédiation pure mais plutôt dans une approche de gestion globale du risque. Ensemble avec le contrôle interne, le responsable sécurité, la direction financière et le chef d'entreprise, nous intégrons la dimension du risque qui suppose une cohérence entre des mesures de prévention, de protection et de financement. S'il n'y a pas d'assurance appropriée, il existe d'autres solutions comme le montage de captives d'assurance, etc.

Qu'est-ce qu'une captive d'assurance ?

C'est un mécanisme d'optimisation par lequel les primes d'assurance ou celles d'un ensemble dont l'entreprise a la maîtrise sont logées dans une compagnie d'assurance ou de réassurance possédée ou contrôlée par cette entreprise, un peu comme si on mettait des primes, de l'argent de côté, dans un fonds en cas de sinistre. On ne peut pas faire ses provisions de propre assurance car elles ne sont pas déductibles mais on peut les externaliser. De grands groupes procèdent ainsi. Cela permet une mutualisation et une maîtrise de ces fonds si tant est que l'on puisse identifier et quantifier le risque. Ainsi a-t-on la maîtrise de ce type de financement, utile quand on se trouve face à des risques mondiaux et complexes.

Le risque informatique a beaucoup évolué.

D'abord le métier de courtier d'assurance a beaucoup évolué avec la globalisation. Les clients qui interviennent au niveau international ont besoin de réponses adaptées.

Je dirais qu'il n'y a pas que les entreprises qui interviennent au niveau international qui sont concernées mais aussi celles qui restent sur le territoire français mais dont les données se retrouvent à l'étranger.

Tout à fait, les systèmes d'information ont complètement évolué. Auparavant, nous avions des systèmes fermés, avec

des données stockées dans un bunker. La question portait sur la protection périmétrique, la cryptographie, etc. Aujourd'hui, le cloud se développe, comme les systèmes interconnectés. L'informatique professionnelle et personnelle se confondent de plus en plus. Les comportements changent. On s'étale sur Facebook et sur Twitter. La législation a également beaucoup évolué. Elle s'internationalise de plus en plus, notamment sur la protection des données personnelles. Nous avons donc une infrastructure éclatée avec des risques multiformes alors que la réponse en assurance reste encore très traditionnelle, avec des offres « sur étagère » qui couvrent l'informatique, pas nécessairement l'information. Cela reste souvent inadapté. Mon travail consiste à aider mes clients et les compagnies d'assurance à affronter ces évolutions. Les assureurs ont des obligations réglementaires de « solvency » qui consistent à maîtriser leurs engagements. Leur exposition aux risques aujourd'hui n'est plus seulement physique et matérielle, elle peut être immatérielle et mondiale. Prenons l'assurance d'un risque comme le virus informatique, comment peut-on le maîtriser, le modéliser alors que le virus mondial peut impacter une multitude de clients ? Cette mutualisation n'est plus possible. Ce risque n'est donc plus assurable car il s'agit d'un risque sériel, diffus et multiple. C'est un peu la même chose pour un assureur en responsabilité civile aux Etats-Unis face à une class action. Pour résumer, nous sommes face à une infrastructure mondiale qui explose en volume, une législation qui réclame de plus en plus de sécurité, des engagements financiers qui peuvent se cumuler en raison du risque sériel. Aujourd'hui, il y a peu d'assureurs et ceux qui acceptent d'assurer le risque immatériel ont une double caractéristique : ils ont une capacité financière qui leur permet de supporter de tels sinistres et quelques réassureurs pouvant lisser le risque au niveau mondial, et un savoir-faire qui leur permet d'avoir une capacité de compréhension et de connaissance du risque. Pour déployer ces offres, les compagnies d'assurance ont besoin de courtiers spécialisés qui connaissent les problématiques de manière à les anticiper et à les gérer pour leur compte.

« Celui qui achète de l'assurance dans l'entreprise n'est pas forcément le meilleur interlocuteur pour acheter une assistance en matière de politique de risques ou de couverture de risques dédiée aux systèmes d'information. »

Pascal Lointier que j'avais interviewé me disait que les courtiers représentent le maillon faible de la chaîne car, pour la plupart, ils ne connaissent pas les risques immatériels.
Je l'ai également observé, mais on peut dire la même chose des risques très complexes (aviation espace, environnement, médical…). J'ai travaillé au sein de grands courtiers comme Marsh, le premier mondial, Gras Savoye, le premier français, et on voit que les assureurs manquent de relais sur ces risques. Par ailleurs, celui qui achète de l'assurance dans l'entreprise n'est pas forcément le meilleur interlocuteur pour acheter une assistance en matière de politique de risques ou de couverture de risques dédiée aux systèmes d'information.

Ce serait plutôt le juriste ?
Cela dépend des métiers et de l'entreprise. Si celle-ci traite beaucoup de données personnelles, comme par exemple les données de santé, son patrimoine informationnel est fortement régi par des règles de droit et le juriste sera donc la bonne personne en raison de la dimension de responsabilité. Si la société gère des échanges dans le monde de la finance, l'interlocuteur sera plutôt le financier. Il envisagera des pertes occasionnées du fait de l'indisponibilité du système d'information. Dans des environnements très technologiques, ce sera plutôt le responsable informatique ou le responsable de la sécurité informatique qui se penchera sur le financement du plan de secours. Il n'y a donc pas un modèle unique. De même, il n'y a pas de réponse unique pour le choix de l'assureur, car le secteur est très spécialisé. Hiscox s'adresse plutôt aux PME et aux professions réglementées, Ace aux grandes entreprises et à l'industrie, Chartis aux institutions financières, etc.

La question de l'assurance se pose-t-elle pareillement pour les collectivités publiques ?
J'ai beaucoup travaillé sur la dématérialisation et l'informatique publique. Les collectivités publiques ont autant de risques et de besoins de financement que le secteur privé.

En 1998 dans Expertises, vous constatiez déjà un glissement du risque de l'informatique vers celui de l'information. Il semble que cette tendance que vous décriviez soit largement confirmée et qu'il convienne de l'envisager sous l'angle du patrimoine informationnel de l'entreprise d'un point de vue juridique et économique. Etes-vous toujours d'accord avec cette affirmation ?
Bien sûr. Auparavant, l'approche était très technique sécuritaire. Mais deux phénomènes que nous n'avions pas vu venir ont modifié la donne : l'internet, qui a fait éclater toutes les frontières, et l'uniformisation des technologies induite par la communication entre les systèmes, avec l'utilisation de normes, de protocoles. Cela génère un niveau de risques partagés car la norme sert à mettre tout le monde au même niveau. En plus de l'évolution de l'infrastructure, un autre point qu'on ne mesurait pas en 1998 est l'usage, la fusion entre l'informatique personnelle et professionnelle. Le risque informationnel constitue donc la contrepartie du développement de l'information. Un risque est toujours la contrepartie d'une opportunité. Il faut accepter ce risque, le gérer et le financer quand cela dysfonctionne.

Oui mais le risque informationnel échappe à la quantification.
C'est un point qui a vraiment évolué. A l'époque de la méthode Marion, on regardait le tryptique : accident – erreur – malveillance. On avait une vision probabiliste, à savoir qu'on envisageait ce qui pouvait arriver. Puis lorsqu'on s'est intéressé au patrimoine informationnel pour le qualifier et le quantifier, on a davantage raisonné en termes de disponibilité du système, d'intégrité des traitements, de confidentialité des données et de traçabilité des opérations. On est passé à un mode déterministe, qui aboutit à se demander à quoi sert le

système d'information. On ne s'occupe plus de savoir si l'indisponibilité est la conséquence d'un accident, d'une erreur ou d'une malveillance mais si cette indisponibilité occasionne des conséquences graves, moins graves ou faibles. Nous sommes passés du risque de l'informatique au risque à l'information. Donc pour éviter cette indisponibilité, l'entreprise va mettre en place des solutions informatiques de back-up mais aussi humaines, des procédures organisationnelles. Nous sortons donc de la seule problématique informatique pour entrer dans la gestion de l'entreprise ou de la collectivité publique. Nous sommes passés de la gestion des risques à la gestion par les risques. Dans le premier cas, on envisage des solutions techniques, dans le second cas on met en place une organisation du personnel, des process mais aussi des mesures d'accompagnement. On était auparavant dans la sécurité informatique avec des plans de secours, aujourd'hui on met en place des plans de continuité d'activité. Il s'agit de gouvernance, non plus au sens informatique, mais stratégique, financier, opérationnel et de communication en cas d'événement quel qu'il soit.

« On ne s'occupe plus de savoir si l'indisponibilité est la conséquence d'un accident, d'une erreur ou d'une malveillance mais si cette indisponibilité occasionne des conséquences graves, moins graves ou faibles. »

Concrètement, comment fait-on pour quantifier ce risque ?

D'abord des évolutions ont été apportées au niveau des normes IFRS et on commence à savoir comptabiliser l'immatériel et le traduire dans les documents comptables. Il existe par ailleurs des outils et des méthodes de quantification du risque direct :tout n'est pas compliqué, comme les coûts de reconstitution des informations, ou le financement du départ en secours si le sinistre est matériel. S'il s'agit d'un sinistre logique, on sait combien peut coûter de dépolluer les systèmes, etc.

Et les données ?

Sur les données, c'est en effet plus compliqué. Avec les assureurs, j'ai monté des programmes mettant en place des indemnisations forfaitaires. Nous avions inventé pour un hébergeur de données un contrat d'assurance qui partait du principe qu'un mégaoctet égal un euro. Cette approche permet d'aller jusqu'à 5 à 6 millions d'euros pour une indemnisation quasi automatique, même si ce n'est pas tout à fait conforme aux principes indemnitaires de l'assurance. Il est possible de rédiger un contrat d'assurance sans qu'il y ait un risque de qualification d'enrichissement sans cause du client.

L'autre approche porte sur la perte de chances, de confiance ou de clientèle (les américains appellent cela le « churn »). J'ai l'exemple en tête d'un laboratoire qui effectue des essais cliniques. Les données informatiques issues de ces essais peuvent être détruites ou inutilisables ce qui obligerait le laboratoire à recommencer sa campagne d'essais. Il peut ainsi perdre un ou deux ans sur l'autorisation de mise sur le marché d'un médicament. Comment calculer cette perte de données ? Est-ce sur la base de deux ans de chiffre d'affaires ? Cela peut constituer une base contractuelle car il n'est pas interdit de créer sa propre métrique. C'est un contrat au cas par cas qui évolue en fonction de la technique ou de la législation. Par exemple, avec la législation sur les failles de sécurité, on se pose la question du financement de la notification des failles. Qui va payer l'appel ou l'envoi de courrier aux clients par l'entreprise ou par un prestataire. Dans le cas de Sony, l'opération avait été réalisée par Chartis et par Affinion, un couplage d'un contrat d'assurance et d'un contrat de service. En fin de compte qui va financer cette prestation ?

Est-ce difficile de répondre à cette question ?

Il faut l'évaluer. Si je prends un exemple simple : une entreprise qui traite 200 000 données personnelles par jour susceptibles de subir une violation de sécurité. On va donc avoir autant de personnes à contacter en 24h. Qui est capable en si peu de temps de mobiliser un plateau d'appel, posséder la liste des personnes, avoir un script prêt et qui a les moyens de le faire, pour un coût unitaire entre 20 et 50 € ? Par conséquent, l'assurance est devenue un service, ce n'est plus un produit. Elle a sa pleine efficacité si elle est associée à des solutions. On est passé d'un mécanisme purement indemnitaire à un mécanisme qui permet la protection du patrimoine informationnel, de l'image, de l'e-business, etc.

L'e-réputation, cela ne doit pas être simple à assurer ?

La question est d'abord celle du comment l'entreprise contrôle sa réputation ? Quel est son niveau de réactivité ? Est-ce qu'elle doit réagir ? Si l'entreprise décide de ne rien savoir sur ce qu'on dit d'elle sur le net, je me demande si elle trouvera un assureur pour garantir un tel risque ou alors ce sera très cher avec peu de garantie. En revanche, si des dispositifs sont mis en place, l'assurance devient, le jour du sinistre, le mode de leur financement. Cela servira uniquement en cas de besoin. Il n'y aura pas de discussion sur la quantification car on saura ce qui a été dépensé. On pourra parfaitement écrire dans le contrat que l'assurance financera, de manière forfaitaire, une reconstitution de réputation. Mais si rien n'as été prévu, rien ne se passera.

Il convient donc d'anticiper les situations et les scénarios possibles.

Les scénarios possibles, les mécanismes pour permettre la continuité de l'activité et maintenir la réputation et la mise en place de solutions financées par l'assurance. Financer le plan de secours est aujourd'hui assez simple, à condition qu'il ait été bien mis en place. Ces changements induisent également un changement d'interlocuteur dans l'entreprise et la réponse à la question de savoir qui est responsable du patrimoine informationnel.

Est-ce que les assurances ont tenu compte de cette évolution dans leurs offres ?

Depuis peu oui, sous l'impulsion des travaux menés par le Clusif, le Cigref qui ont beaucoup réfléchi sur la notion de patrimoine informationnel. Ils ont travaillé sur les normes, notamment ISO 2700x et 17799, sur les règles de place Bâle II et Solvency, mais ils ne sont pas allés jusqu'au bout de la réflexion concernant les mécanismes de financement des risques. Aujourd'hui, la capacité du marché à financer ces risques est relativement faible. On peut trouver des garan-

ties jusqu'à 100 millions d'euros et plus, mais rapportés à des sinistres majeurs, nous ne sommes pas au niveau souhaitable.

En dehors de la capacité financière, les contrats d'assurance ont-ils évolué ?
Il y a relativement peu d'acteurs, et ils sont plutôt en position dominante. Mais en même temps, la concurrence commence à se développer et le marché se segmente. Il faut donc connaître les acteurs, avoir leur confiance, souscrire des garanties pour des risques dans un contexte où la confiance existe des deux côtés.

Quid des conséquences de l'évolution de la fourniture de logiciels ?
De passer d'une police de responsabilité éditeur de logiciels à une police de fournisseur de logiciels en mode SaaS qui héberge les données dans le cloud, c'est passer à un autre schéma, une autre exposition aux risques et un autre type d'indemnisation. Aujourd'hui, des éditeurs de logiciels en mode SaaS sont encore couverts par une police d'éditeur classique. Tant qu'il n'y a pas de sinistre, tout va bien, mais ce n'est pas au moment du sinistre qu'il faut discuter de la police et de son efficacité. D'autant que le système d'information s'étant ouvert, le risque est plus fort tant en probabilité d'occurrence qu'en impact.

« On est passé d'un mécanisme purement indemnitaire à un mécanisme qui permet la protection du patrimoine informationnel, de l'image, de l'e-business, etc. »

Quid en matière de cloud computing ?
Il ne faut pas oublier que le client qui fait héberger ses données en mode cloud reste le responsable du traitement de données personnelles, et donc de sa sécurité. Dans certains cas, soit ils ne disposent plus de leurs données, soit ils risquent d'avoir des problèmes de maîtrise de la sécurité, en particulier dans leur environnement réglementaire métier. Si on explique bien la situation aux assureurs, il est possible qu'ils ne prennent pas le risque de garantir l'atteinte aux données dans un environnement cloud. S'ils le prennent sans savoir, le problème se posera au moment du sinistre.

Le cloud computing pose-t-il un problème à l'assurance ?
La vraie question posée à l'assureur par le cloud est celle de la réversibilité. Puisque les données ont été externalisées, cela relève de la responsabilité de l'hébergeur, avec les limites contractuelles de responsabilité et l'impact de la force majeure. Si les données sont devenues indisponibles, qui va en supporter la charge financière ? Pour l'assureur, le cloud représente donc une aggravation du risque en raison de l'externalisation des données. Cela va se compliquer si l'atteinte aux données a un impact sur l'activité. Quid en cas de contrôle fiscal et que la comptabilité est perdue dans le cloud, même chose si une autorité de contrôle réclame les messages électroniques, etc. Mais selon moi, que les données soient dans l'entreprise ou en dehors, cela reste les données de l'entreprise. Certains vont jusqu'à affirmer que les données externalisées sont parfois mieux sécurisées car elles sont stockées chez des professionnels : aggravation ou minoration du risque ?
L'autre grande difficulté réside dans l'assurance des opérateurs de cloud car ils mettent tous leurs oeufs dans le même panier. J'ai eu à traiter de ce cas. On avait proposé une garantie forfaitaire au giga et il revenait au client d'estimer le montant de son exposition en fonction de la nature des données, que lui seul connaissait. On avait imaginé un contrat de groupe qui prévoyait des lignes de garantie en fonction de cette exposition. On avait également mis en place un tel montage pour la signature électronique. Il y avait des certificats de signature plus ou moins robustes, suivant qu'ils servaient à signer un acte simple ou un acte notarié. Il y avait donc des garanties associées à ces différents certificats. L'imagination est à pouvoir... à condition de comprendre de quoi on parle.

Vous vous êtes intéressé à la protection du secret des affaires. La situation actuelle est-elle satisfaisante ?
Du point de vue du juriste, quand on voit comment on a tordu la notion de l'abus de confiance, dans la décision Michelin, on regrette de ne pas avoir suivi Pierre Catala et ses travaux sur la qualification juridique de l'information. Aussi tout ce qui va vers une définition plus précise et plus normée de l'information et qui n'oblige pas les magistrats à réinventer le droit me convient. Seulement, cela ne règle pas la question de la protection au plan technique.

La proposition de loi de Bernard Carayon prévoit une réponse pénale au problème de la protection du secret des affaires. Est-ce une bonne réponse ?
La réponse pénale est plutôt un aveu d'impuissance technique. On a du mal à gérer, à quantifier, et à protéger, alors on préfère sanctionner au cas où on attrape un présumé coupable. La question de la protection du secret des affaires pose un problème qui va au-delà de l'informatique qui est celle de la protection de l'immatériel dans un monde ouvert où la dématérialisation a rendu la duplication des objets informationnels extraordinairement facile. Peut-être existe-t-il une troisième catégorie entre les choses et les personnes qui serait l'information. Auparavant, on fabriquait des objets pour améliorer la vie des personnes. Puis la dématérialisation a créé des objets sortis du monde réel, et a transformé les personnes en données personnelles. Nous sommes donc dans un monde post-industriel avec une économie numérique qui continue de raisonner sur des choses et des personnes en traitant de l'immatérialité plutôt que de ses aspects contentieux ou déviants. Tout le problème vient de là.
Je travaille sur la sécurité des systèmes d'information. Sécurité et systèmes, je vois à peu près ce que c'est, mais je n'ai pas de définition de l'information. Finalement, qu'est-ce que la notion de patrimoine informationnel ? C'est une tentative d'encapsuler de l'information dans une vision patrimoniale au sein du monde numérique.

Que mettez-vous dans le patrimoine informationnel ?
J'y mets des objets informationnels multiformes, des traitements et des flux, alors que le patrimoine physique est immobile. Aujourd'hui, la vraie question est celle de la disponibilité de ces flux et de l'intégrité de ces traitements.

Propos recueillis par Sylvie ROZENFELD