

Profession : chasseur de risques

Daniel Remy est souvent présenté comme le « risk hunter » français. Depuis plus de vingt-cinq ans, cet ancien instituteur touche à tout ou « autodidacte confirmé » comme il se définit lui-même, n'aime rien plus que traquer les risques qui visent les personnes et les entreprises... Ce passionné, consultant et auteur de nombreux articles ou ouvrages sur le sujet¹, nous explique son métier.

Comment devient-on expert du risque ?

Daniel Rémy : On le devient par hasard, dans un premier temps, par passion ensuite. C'est un véritable travail d'investigation avec son côté ludique, à la manière d'un joueur d'échecs... L'anticipation est le maître-mot : il faut toujours avoir au moins un sinon plusieurs coups d'avance sur l'adversaire ou, si j'ose dire, sur la fatalité. Une fatalité qui cache trop souvent des erreurs de diagnostics ou pas de diagnostic du tout. Malheureusement, il n'existe pas de véritable école, en dehors des risques technologiques, industriels ou naturels, où les ingénieurs sont légion. Pour autant, on voit bien que quel que soit le bagage scientifique affiché par ces spécialistes, les accidents et catastrophes majeures sont fréquents (AZF, crashes d'avions, marées noires, déraillements, etc.). La meilleure école est celle du terrain, comme toujours... Mais il y a là une explication précise : c'est que, en matière de gestion de risques, le facteur humain représente à lui seul, au bas mot, quatre-vingts pour cent du risque. Et le facteur humain, à ma connaissance, personne n'a encore jamais su le mettre en équation, pour le simple motif qu'il est souvent irrationnel. Qui, avant le 11 septembre 2001, aurait pu faire entendre autour de lui que deux avions de ligne pilotés par des kamikazes étaient susceptibles de venir se jeter sur les Twin Towers ?

Des actes de malveillance, de sabotage, d'espionnage industriel, de concurrence déloyale ou de déstabilisation (lettres ano-

nymes, rumeurs, campagnes de désinformation, chantage...) ne se traitent pas de la même manière qu'un risque purement technologique ou industriel (bogue informatique, résistance des matériaux, risque de pollution, risque incendie...). Pourtant, même dans cette typologie de risques, il convient toujours de se poser la question de savoir si l'intervention de l'homme, qu'il soit défaillant ou malveillant, n'est pas de nature à aggraver très sensiblement le risque.

Le cas d'AZF à Toulouse est exemplaire : quand toutes les expertises privilégient la thèse d'une négligence ou d'une cause inexplicquée, on évitera soigneusement de faire valoir qu'un acte de malveillance, ici comme ailleurs, aurait parfaitement pu produire les mêmes résultats. Est-ce pour autant que ce risque a été pris en compte et les mesures de protection mises en œuvre... ?

La gestion des risques est un métier qui exige la pluridisciplinarité, mélange de sciences et de psychologie, beaucoup de logique et de rigueur, d'imagination, d'intuition, de curiosité et, surtout, une grande expérience. En outre, le fait d'être également, par ailleurs, un chef d'entreprise me permet d'intégrer, dans mon analyse, des paramètres tels que : gestion d'image, plan de communication, partenaires sociaux, plan marketing, retour sur investissement, etc.

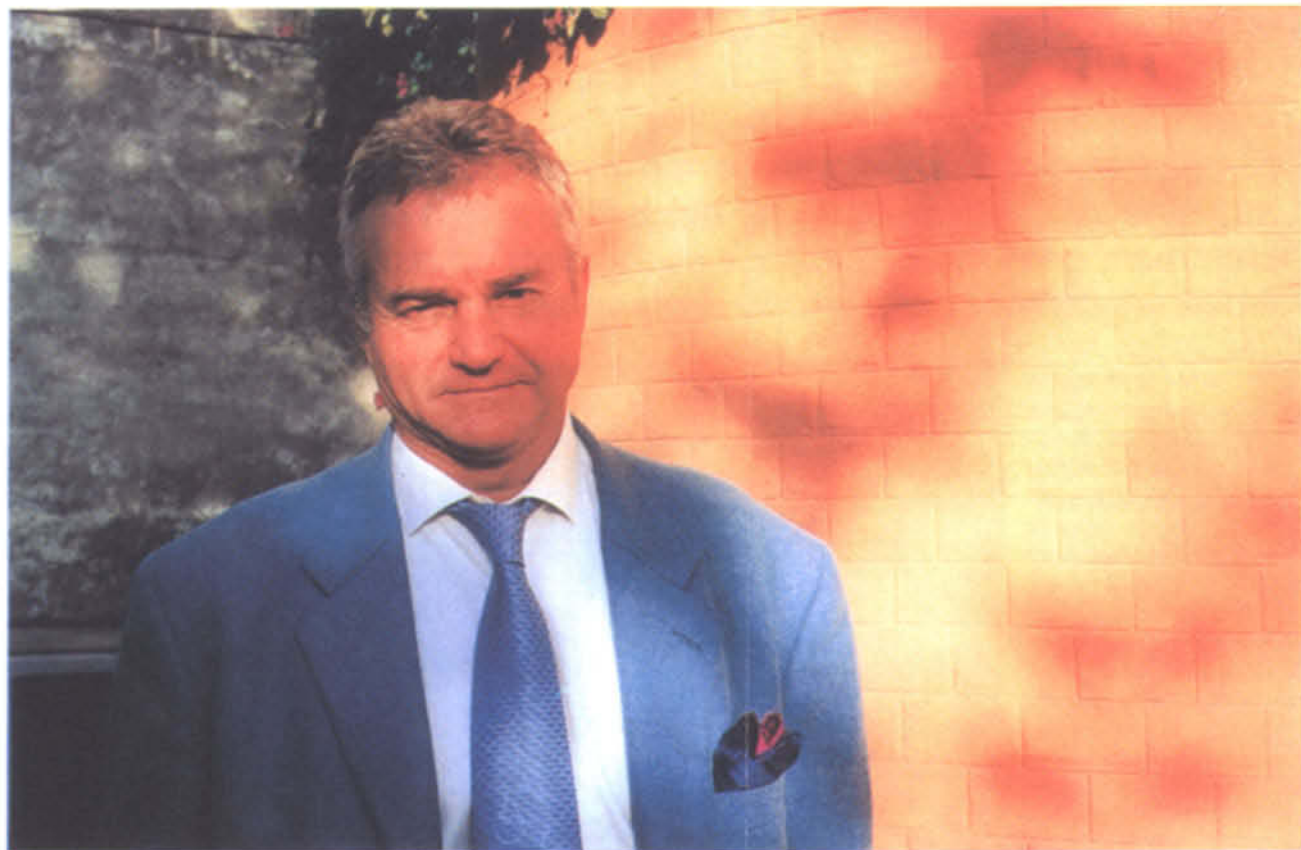
Vous avez débuté dans la sécurité en créant la première entreprise spécialisée dans la protection des personnalités. C'est pourtant très différent de la protection

des entreprises, non ?...

D.R. : Pas du tout ! Au contraire, c'est précisément là où j'ai le plus appris. Quand, confronté aussi bien aux attentats conduits par Action Directe que par des terroristes originaires du Moyen-Orient, vous avez en charge la protection du président d'un grand groupe, de sa famille, de son domicile, de ses résidences secondaires, de son entreprise (siège, filiales) et de ses déplacements en France ou à l'étranger... Croyez moi, avec ce type de risque, vous n'avez pas le droit à l'erreur. Le grand public ne retient de cette activité que la part de vernis : souvent de jeunes et solides garçons hyper-entraînés, ignorant la peur. En fait, l'essentiel de la sécurité repose sur des mesures de sûreté qui se situent très en amont, comme, par exemple : des missions de renseignement, de détection et de surveillance électroniques, d'investigation et de contre-observation, ou la mise en œuvre de multiples dispositifs de protections mécaniques et, surtout, de procédures particulières très strictes, à destination de tous les acteurs concernés.

Enfin, comme pour une entreprise classique, il ne peut exister de bonne sécurité qui n'ait fait l'objet, au préalable, d'une bonne perception de la menace, d'une analyse détaillée des risques assortie d'un bon diagnostic. Comme on le voit, la sécurité est au hardware ce

¹ - « Qui veut tuer la France ? », Editions Jacques Grancher.



que la sûreté est au software : l'un ne peut fonctionner sans l'autre...

Tout ceci paraît logique, mais les entreprises ne disposent-elles pas, en interne, d'un risk-manager ?

D.R. : Bien sûr que si ! Mais cela n'est en rien incompatible avec l'activité d'un consultant extérieur : pour des raisons de culture et d'expérience, comme on l'a vu, mais aussi parce que celui qui vient de l'extérieur bénéficie toujours d'un « œil neuf » qui lui permet bien souvent de repérer les faiblesses ou les failles du dispositif de sécurité quand le « spécialiste-maison », par la force de l'habitude, a fini par ne plus les voir... En outre, le responsable sécurité qui passe volontiers pour l'empêchement de tourner en rond, limite paranoïaque, verra sa copie mille fois corrigée par le directeur financier de l'entreprise. A l'inverse, le consultant ne rend compte qu'au président, sans se soucier de plaire ou de déplaire : c'est aussi à cela que l'on reconnaît sa qualité...

Quelles sont les principales menaces qui pèsent sur l'entreprise ?

D.R. : Pour ma part, le risque majeur, pour une entreprise, est celui qui est susceptible de porter atteinte à son image. Viennent ensuite, pêle-mêle, les risques de déstabilisation (lobbies), d'espionnage économique, de concurrence déloyale, de contrefaçon, d'escroquerie, sans oublier, bien entendu, les risques plus « généralistes » : risques politiques, économiques, industriels, environnementaux, sociaux... Dieu merci, le terrorisme, le racket et le chantage demeurent encore marginaux.

Croyez-vous qu'aujourd'hui, les chefs d'entreprise soient davantage sensibilisés aux risques qui pèsent sur eux ?

D.R. : Malheureusement, non ! Il faut toujours un accident grave pour rappeler aux chefs d'entreprise que ce qui est arrivé à l'un de leurs concurrents peut leur arriver aussi. Malgré cela, celui qui n'a jamais été touché durement aura toujours tendance à privilégier la lecture des cours de bourse et celle des comptes d'exploitation, oubliant un peu vite qu'un sinistre majeur, même avec une bonne couverture d'assurance, peut altérer très

sensiblement l'image comme les résultats de l'entreprise...

Les chefs d'entreprise se donnent-ils les moyens ? Et peut-on contrer tous les risques ?

D.R. : Manifestement, non. En premier lieu, pour les raisons que j'indiquais précédemment. Ensuite parce que, ayant délégué la fonction de sécurité au sein de l'entreprise à un responsable (au plan juridique et judiciaire...) désigné, le chef d'entreprise considère qu'il n'a plus à s'en soucier : c'est une erreur. Même si la sécurité à cent pour cent (ou le « risque zéro ») n'existe pas, cet argument sert souvent de prétexte à ne rien faire du tout, voire le minimum. Cette approche est préjudiciable car mon expérience m'a toujours appris qu'avec des moyens limités on pouvait atteindre des niveaux de sécurité et de sûreté satisfaisants. Ceci suppose que l'entreprise ait parfaitement identifié ses risques et ait mesuré, pour chacun d'entre eux, la réalité du préjudice encouru en cas de sinistre : c'est

précisément le travail du consultant...
fguinochet@medef.fr