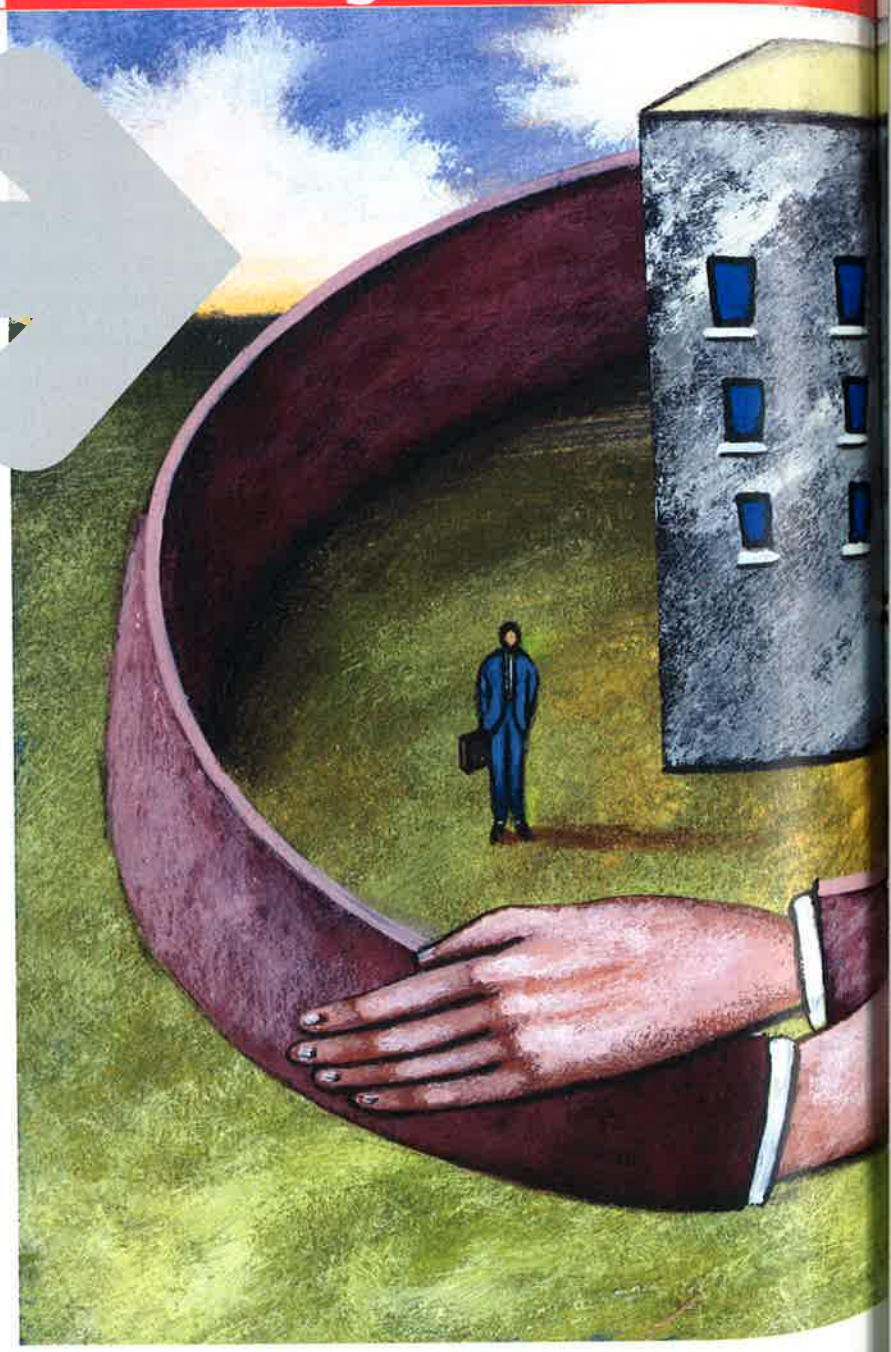
Risk Management

The key ... and three thought-provoking strands

Now that a Risk Manager certification process is underway, it is a good time to cast a look back at the basic principles underlying any ongoing Risk Management system. Into the mix we'll also throw some seedbed thoughts about how best to set up a systematic risk treatment process. Risk Management is a vital remit within any organisation but like any other important mission it calls for proper recce of the terrain beforehand. The sole aim of this article is to fuel this evolving, forward-looking view.



FRANÇOIS SETTEMBRINO
RISK MANAGEMENT
FERMA

It was over a half a century ago that the inventors of Risk Management set out to build up the system. Starting from scratch, they needed to call on all their courage to strike off down an unbeaten path. The hardest hurdle was to eschew the knee-jerk habit of considering only insured or insurable risks as their raw material. The future has proven them quite right here, since the «new risks» perceived over time are not all insured or even completely insurable.

ILLUSTRATION STOCK

Let's concentrate first on those principles that, in the eyes of these trailblazers, were the sine qua non of any enforceable Risk Management system;

- Top management has to be involved across the board in the whole implementation process. It is up to them to kick things off; it is up to them to allocate enough resources and it is also up to them to keep the whole thing moving in the right direction thereafter: such a vital process cannot be left to its own devices; it needs to be stoked up permanently to keep it going.

- According to the size of the undertaking concerned, its type of organisation, geographical location, its objectives and operating procedures, Risk Management will be more or less centralised.

- For the sake of simplicity, current literature on this subject continues to speak of the Risk Manager. In fact it might be better to speak of the Risk Management entity because no one can deal with this task single-handedly in a large organisation. This caveat made, we can continue to use the term «Risk Manager» for ease of comprehension.

- Risk managers need to be slotted into the structure; the pioneers soon cottoned onto the fact that fitting them into one of the undertaking's component departments, the financial department for instance, would rob them of all freedom of action.

They therefore stood in need of a «staff» function as the only way of ensuring independent reporting to top management. What is still astonishing even today is that they generally obtained this position … back then. Today, however, few companies still take this into consideration. What raises the hackles of too many executives is the thought that anyone within their organisation should have the right to come up with criticisms and give out warnings. This runs counter to the complacent navel gazing that has all too often taken hold within the highest spheres.

■ They therefore needed to be invested with a certain authority to break through this inertia and be able to work properly; our pioneers had to win the right to cull company-wide information and obtain answers to their questions. Right from the word go it was a given that many of the problems to be dealt with would take in different disciplines, and the best way of tackling them was by way of multidisciplinary groups under the eye of the Risk Manager. In both cases, whatever might be the outcome of their enquiries and discussions, they would be subject to top management or the board, which then takes the pertinent decisions and imposes the complementary duties. It is undoubtedly they who should take the big decisions, since, as far as Risk Management is concerned, it is the managers who manage and it is they who are held liable for these decisions.

■ One of the roles devolved on the Risk Manager, or on the Risk Management entity, was internal education and awareness-raising on this matter. When this duty was exercised *vis-à-vis* top management it was usually trouble-free. As already pointed out, it is they who have kicked off the whole process and they are perfectly aware per se of its importance. People on the ground, being closer to the real problems, were quite naturally hungry for information and training and were therefore very interested in the matter. The most recalcitrant were usually middle-management, caught between the devil of their objectives and the blue sea of the best possible yield. It was therefore this group that had to be most closely monitored, with additional newletters and seminars. Permanently developing electronic resources have also been a great help in this matter. As a knock-on effect of all this, it is now incumbent on the Risk Manager and his/her team to engage in continual top-up training to keep up with the pace of events.

WHAT RAISES THE HACKLES OF TOO MANY EXECUTIVES IS THE THOUGHT THAT ANYONE WITHIN THEIR ORGANISATION SHOULD HAVE THE RIGHT TO COME UP WITH CRITICISM AND GIVE OUT WARNINGS

Take away any of the abovementioned factors and a true Risk Management becomes practically impossible; this is in fact what has happened. When the trailblazers left the field they were seldom replaced by viable successors. Management and managers began to turn their interest only to the market value of their organisations; mergers and takeovers became investors' cynosures, and risks gradually slipped out of the picture, with financial manoeuvres now hogging the attention. Risks were still there; managers increasingly turned a deaf ear and a blind eye to them but risks nonetheless were continually brought back to the urgent attention of one and all. From Enron to Fukushima, taking in the subprime crisis

along the way, the list of disasters is harrowingly long and striking.

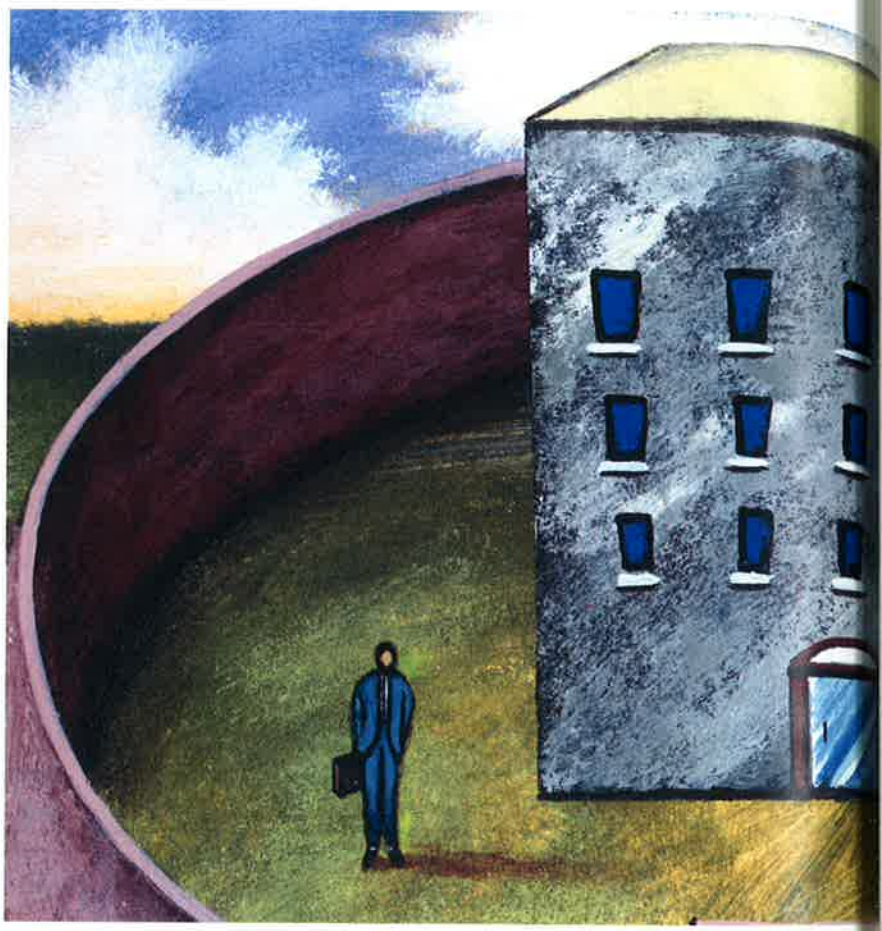
There is now an urgent need to turn the clock back to the good practices of those early days. Today's certification endeavours are a step in the right direction. At the same time managers now need to be re-educated because without them onboard all will be in vain. There is still plenty of work ahead of us!

All organisations are «one» and hence unique. It is for this very reason that there has never been and will never be a one-size-fits-all Risk Management model. On the basis of the abovementioned principles, which sketch out between them a well-structured «keynote», each organisation then needs to adapt them to its profile, its procedures, financial, political and geographical constraints and its own particular culture. This is a labour of Sisyphus, calling for continual rethinks; it is for this very reason that Risk Management is such a thrilling job. It would be equally useful to review the education possibilities and availabilities to avoid spreading things too thin.

THERE HAS NEVER BEEN AND WILL NEVER BE A ONE-SIZE-FITS-ALL RISK MANAGEMENT MODEL

Now let's look at three thought-provoking strands to give us a better grasp of the matter in hand. Each one of these strands would rightfully call for an in-depth analysis by specialists in each case. The outline sketch to follow does not pretend to be at all exhaustive but rather kindle the necessary interest for this all-out research effort in the future.

● To start with, let's look at what has come to be dubbed Cyber Risk. Attacks are continually being launched against all comers. It is not only companies and other organisation that have been targeted; no one is immune from this threat. Humble individuals like ourselves are besieged by just as much attention as the major firms, whether to track our buying habits, spy on our intimate relations or plumb our financial capacities, our banking relations and almost anything else. All this is met with almost complete indifference; nearly everyone is aware of the dangers of the social networks but nearly everyone is almost equally *blasé* about them, even while new risks are being brewed that will only be discovered too late. Not to speak of companies and even governments, since almost every day we discover that one of them has proved incapable of setting up sufficient or efficient safeguards. The skill of the wrongdoers is always to remain one step ahead of their victims; so far do they push their advantage that they secretly set up a permanent presence inside the systems they have penetrated, allowing



them to keep track of everything going on therein and then choose their moment or target for a surprise attack. Should we then drop our guard and throw in the towel? Surely not; on the contrary, defences and safeguards need to be kept under permanent scrutiny; the quicker any intrusion is discovered, the faster the response. User education is crucial, making sure they never get weary and forget the security rules that slow down their work. It is no longer purely an IT question. The wider takeup of teleworking and the proliferation of smartcards are blurring the distinction between work and social networks; inroads can now be made where least expected and supposedly confidential documents are sometimes so little secret that reaching them is only too easy. Here we find a typical Risk Management picture, where the problem needs to be tackled in depth and in common, with top management deciding on the strategy to be adopted and the actions to be taken. Everyone knows about the existence of «backdoors» which have been surreptitiously left in the operating system of any computer, allowing anyone with the necessary keys to bypass all authentication systems and infiltrate the ostensibly secure computer. Google, Outlook and co are no exceptions to this rule. Worse still is the anonymous sharing system Darknet. This allows communication to be set up unbeknown to any surveillance, spying or communication-intercepting system. It has been welcomed with open arms by internauts who have been gagged, persecuted or simply coerced by certain dictatorial powers; this is their only way of making their fate more widely known and communicating freely. But the same system is also a boon for *mafioso* networks, allowing them to carry out their activities with total impunity. To date Darknet has remained impenetrable and the encryption used has withstood all efforts to break it. The tragedy lying behind this brain-teaser is that it will soon render obsolete part of the famous, staggeringly technical spying activities that have only just hit the news, hogging international headlines recently. The poacher poached ... But for our purposes here, risks have thus become uncontrollable because we no longer know how to find out who is fuelling darknet nor what it might filch unbeknown to one and all: manufacturing secrets, inventories of all sorts, clients, suppliers, strategic products. If there is any way of stopping this now it is not yet known and will call for some sharp thinking. But who will take this on? That is the question...

RISK MANAGEMENT ACROSS THE POND HAS TIMIDLY REINSERTED A CONCERN FOR STAKEHOLDERS BACK INTO THE PROCESS

● The second strand we are going to look at concerns human capital and the «persons » making it up; this human capital is all too often mistreated or underestimated. It is also curious that their fate has been entrusted to «human resource» specialists. This nomenclature is all too similar to other company resources like raw materials, energy, subcontracting, etc… Likewise, if any human resource should become too expensive or complicated or unwieldy it is simply replaced. It is for this reason that personnel is treated like coal; if it is too expensive it is replaced or switched to another site with no consideration whatsoever for any concomitant human problems. Witness the stockmarkets, which have always reacted favourably and completely ruthlessly to any restructuring or relocation/offshoring project. At such a moment the human resources boss is no longer the link between management and personnel; he or she is merely the enforcer of higher wills and is bound to make sure this costs as little as possible, with social plans that are tantamount to burials. Why bother about the personnel and protect them under current legislation if all these much more burdensome constraints can be sidestepped by subcontracting or offshoring?

Risk Management across the Pond has timidly reinserted a concern for stakeholders back into the process. These stakeholders are mainly made up by personnel but also trade unions, clientele, partners, suppliers, joint contractors and subcontractors, investors, creditors, without forgetting the taxation authority, or the environment. Among the many who have not been cited figure the competitors. Taken together, or even singly, these stakeholders belong to different classes of vulnerability, such as personal expectations, loss of information, loss of resources, property damage, etc. all of which are worthy of permanent attention. The means of response are legion; one soon sees that this second strand weaves through the firm's whole fabric and also restores to management the position of responsibility it should never have relinquished. As an immediate consequence Risk Management has relearned the difference between the principles of precaution and prevention. Prevention can be exercised only against risks with a measureable probability whilst precaution can be applied only when neither the scope nor probability can be calculated. Any Risk Manager should permanently navigate from one to the other, resorting perforce to resilience whenever things jam up… It is also quite

striking that Belgian welfare legislation has resolutely pushed back the envelope from accidents at work to take in too questions of organisation, relations, harassment and even strayed into the psychosocial domain. It is even more striking that the responsible director can report only to the head of the company with no intermediary and that within his or her duty he or she can be subject to no other. Dealing with a company's human capital in this way is a legal and obligatory demonstration of how Risk Management should work, with direct access to the head of the company.

DEALING WITH A COMPANY'S HUMAN CAPITAL IN THIS WAY IS A LEGAL AND OBLIGATORY DEMONSTRATION OF HOW RISK MANAGEMENT SHOULD WORK, WITH DIRECT ACCESS TO THE HEAD OF THE COMPANY

● The third strand we are going to look at is a real hornet's nest. It concerns the whole concept of «reputation », the visible face of the brand image. All the manuals agree: this value is irreplaceable and is worthy of the maximum defence and protection. But it is so fragile that a simple rumour can bring it crashing down, and building it back up again is always a difficult and sometimes an impossible mission. The doubt always lingers on in people's minds thereafter on the principle «there's no smoke without fire … ». If there is one problem where managers remain jointly and severally the most important stakeholder, it is certainly here. It is therefore a *sine qua non* of good governance, and this in turn brings out its key role in Risk Management. A glance back at the recent Perrier case gives us a salutary example of how things can go wrong. The benzene contamination of its bottled water had been well managed, with an expensive recall of a huge number of bottles, but it was the shilly-shallying of the directors that did most damage. The brand image, and *ipso facto* its value, plummeted and the company was snapped up at a bargain price by another group.

What makes the management of this risk practically impossible at the present time is the fact that it is the managers themselves who muddle the message. In 1976 Emmanuel Todd made the following analysis of the Eastern Bloc: «...a technology-driven society where technology is not used for the good and safety of its citizens cannot last …». Now this is exactly what is happening today, under the bogus banner of globalisation; this serves as *carte blanche* and pretext for doing anything, conditions of slavery generated by offshoring operations, the swamping of all products, especially agrofood products, with additives and

other substances whose danger to health is underestimated or simply denied, declining biodiversity, rampant greenhouse effect … Specific examples are not lacking but are only just beginning to emerge thanks to a courageous few who have refused to be gagged. The best known, by name, are fish farming, adulteration of the food chain by the introduction of false products such as analogue cheese, the horse-meat scandal, food additives used before being proved innocuous, fuelled by the general habits of unhealthy eating, etc. The big industrial groups behind these outrages truly fear nothing. So powerful are they that they instrument their own impunity. The means at their disposal go by the names of lobbies, unscrupulous as long as big bucks

WHAT MAKES THE MANAGEMENT OF THIS RISK PRACTICALLY IMPOSSIBLE AT THE PRESENT TIME IS THE FACT THAT IT IS THE MANAGERS THEMSELVES WHO MUDDLE THE MESSAGE

are in sight, self-seeking scientists, ubiquitous lies to brew up specious opinions that mutually cancel each other out. Health authorities are flooded with such contradictory theories that their watchdog role goes out of the window. How can you expect any Risk Management principles to be enforced in such a context? If industrial ethics does not get back to where it should be, i.e., honest and upright, how can we expect them to correct the hugely-profitable risks that they themselves have generated and only come to light too late?

Let's leave the final word to Stéphane Foucart, for he expresses well the growing disarray of those who believe in Risk Management… « … accumulated knowledge is cast into doubt, contested by mock scientific methods or manipulated by the industries who find it cobbles them … The scientific project is to understand the world; conversely the technical project is to make profit from it … »[1]. But once science plays second fiddle to technology the game rules change and the very idea of precaution disappears forthwith. There is no longer any possibility of bringing a scientific diagnosis into any industrial activity; industry makes sure that any grain of truth gets lost in a mist of pseudoscience producing only uncertainty and ignorance. Whether Risk Management can rise to this challenge only the future will tell. I

[1] La Fabrique du Mensonge. Comment les industriels manipulent la science et nous mettent en danger. Stéphane Foucart, edited by Denoël Impacts, 2013, pages 17 and 18.