THE
HAWKAMAH
JOURNAL

A JOURNAL ON CORPORATE GOVERNANCE & LEADERSHIP

Issue 10
Since the late 1990s risk management has risen steadily up the corporate governance agenda. Yet a sceptical observer of the corporate world might well ask, to what effect? Catastrophic safety failures at Tokyo Electric Power Company (Tepco) after the Fukushima nuclear incident and at BP with the Deepwater Horizon oil spill in the Gulf of Mexico; excessive risk taking by banks and the insurer AIG in the financial crisis; the creation of millions of fraudulent savings and checking accounts at Wells Fargo without clients’ consent; deliberate evasion of carbon emission regulations at Volkswagen; an embarrassing cyber security attack on Deloitte, which advises corporate clients on cyber security – these are just a handful of the more high profile examples of value or reputational damage resulting from poor risk management. So what is going wrong?

In most jurisdictions in the developed world and in many emerging market economies companies legislation and corporate governance codes firmly ensconce responsibility for risk management in the boardroom. The UK’s 2006 Companies Act, for example, requires companies above a certain size to prepare a strategic report for each financial year. This must include, amongst other things, a fair review of the company’s business, and a
description of the principal risks and uncertainties facing the company. In the US quoted companies are required to report extensively in their annual filing of accounts at the Securities and Exchange Commission on the critical risks they face. While the UK and US constitute best practice, the general thrust is little different around the rest of the world.

Meantime, a common feature of governance codes is the assertion that the board is responsible for determining the nature and extent of the principal risks the company is taking to achieve its strategic objectives; likewise that it should maintain sound risk management and internal control systems. Directors are generally required to confirm in the annual report that they have carried out a robust assessment of the principal risks facing the company, including those that would threaten its business model, future performance, solvency or liquidity. Such risks have to be explained, with some description of how they are being managed or mitigated.

The more demanding codes also stipulate that the board should monitor the company’s risk management and internal control systems and carry out an annual review of their effectiveness, and report on that review in the annual report. The detailed work on risk management is usually then carried out by audit and risk committees on which independent non-executive directors are strongly represented. All board directors nonetheless remain collectively responsible for presenting a fair, balanced and understandable assessment of the company’s position and prospects, taking into account the risks being run.

The first area in which many companies fall short of these requirements relates to reporting. From the shareholder’s perspective few annual reports have anything very useful to say about shortcomings that have been exposed by the annual review. This is because directors can use the excuse that to reveal vulnerabilities or failures of risk management would be prejudicial to the company’s interest. More importantly, the level of risk appetite in a given company may be less the product of a conscious board decision than a residual by-product of the business planning process.

Above all, incentive structures within companies and capital market pressures from without can run counter to the demands of judicious risk management. That was certainly the case before the financial crisis. All the big investment banks felt obliged to take on more risk because their chief executive officers knew that to fall behind their competitors in the markets for complex mortgage backed products or leveraged loans would entail a serious career risk. As Chuck Prince, CEO of Citigroup, remarked in July, 2007, on the eve of the credit crunch: “When the music stops, in terms of liquidity, things will be complicated. But as long as the music is playing, you’ve got to get up and dance. We’re still dancing.” This has been widely misinterpreted as a typical example of bankers’ stupidity during a credit bubble. But in reality it was an accurate description of the process whereby institutional shareholders and analysts encouraged excessive risk taking. At the same time any shortfall against earnings expectations could be brutally penalised by a collapsing share price and pressure for the CEO’s departure.

At Tepco there were more formal derogations from good corporate governance practice. The company’s board was cumbersome and dysfunctional, with only two external directors out of a total of 20. There was no board level risk committee. It was striking, too, that when the government in 2002 and 2007 accused the company of false reporting and systematically concealing nuclear plant safety incidents, including radiation leakages, there was little attempt to identify those at fault. The poor response to these governance failures was exacerbated by regulatory capture – a deep seated problem in Japan – where the corporate sector is notoriously cosy with its regulators.
In the case of BP in the Gulf of Mexico, by contrast, distorted incentives were at the heart of the problem. The corporate culture encouraged corner cutting on safety in the interests of short term financial performance. That culture had been moulded by a charismatic and dominating chief executive, Lord Browne, who had departed by the time the catastrophe took place. There was also a failure on the part of the analytical community. Over a number of years a succession of health and safety disclosures pointed to flaws in risk management. These ranged from explosions at BP’s Grangemouth refinery in Scotland and at Texas City, via burst pipelines and gas leaks in Alaska and Azerbaijan to record fines in the US for sundry health and safety violations. Stock market analysts, fixated on a very narrow financial definition of corporate performance, failed to recognise the value destroying potential of non-financial risks. Non-executives and shareholders also failed to pick up the signals and identify the dangerous nature of the culture. This was despite the emphasis in the UK corporate governance code on the need for the board to take responsibility for an organisation’s culture, especially in relation to addressing risk.

All this underlines the considerable difficulties for non-executives in trying to understand what motivates managers and employees at below
board level – all the more so when deception or fraud are involved. At Wells Fargo employees were concealing the opening of new accounts for customers. As with many other corporate scandals and governance failures this was partly the result of excessive pressure to generate results that would boost top executives’ performance related bonuses. While it is too early to be sure who knew what at Volkswagen over the subversive carbon emission software, it may well be relevant that the CEO was desperate to turn VW into the world’s number one car manufacturer. Those who fixed the software may have thought they were helping deliver on this ambitious target.

The mechanics of risk monitoring can also be unhelpful, not least because they may involve work being done in silos. Risk committees are often captured by finance directors who produce elaborate taxonomies and matrices of risk that ignore many of the kinds of risk that can wreck a company. These attempts to outline critical risks rarely include such threats as the CEO overpaying for a hubristic takeover at the peak of the stock market cycle, or becoming more obsessed with the thrill of the chase in the capital markets than with improving the underlying operating performance of the business.

When a finance director is driving the risk committee agenda it is unlikely that the committee will identify the risk that excessive pay for the chief executive is undermining the company’s licence to operate and forfeiting the support of its institutional investors. Nor will it necessarily worry about taking on excessive leverage by buying back shares where such financial engineering boosts earnings or share related bonuses. Or again, a finance director’s matrices will rarely identify the risk that an outgoing chief executive may want to dress up the figures to add a flourish to his or her departure. It would be interesting, too, to know how many of the finance directors who told academic surveys that their companies have forgone profitable investment opportunities to bump up short term earnings had identified the resulting potential loss of market share as a critical risk.

Such omissions have their roots in a principal-agent problem whereby the CEO’s interests are not aligned with those of shareholders. And there are other behavioural and cultural issues relating to risk, which arise from poor tone at the top. It seems intuitively unlikely that a risk committee or board would identify top executives’ dislike of being given bad news as a critical threat. Yet that is often a key component of corporate value destruction. Executive directors may also be reluctant to identify the risks inherent in an internal audit function that lacks effectiveness because of want of support from the top.

The overarching message is that company law and governance codes are all very well, but incentive structures, agency problems and cultural considerations can be huge obstacles to effective risk management – especially when, as in the financial crisis, the capital markets offer short term rewards for excessive risk taking and tough penalties for prudent behaviour.