Keynes’ ‘Animal Spirits’ in the financial markets

Also in this issue
- Black Swans Mean Business
- How Canadian Banks have Managed the Economic Crisis so well
- OTC Clearing Evaluation of the EMIR and Dodd-Frank Regulations and their Impact on IT
- International Financial Supervisory Convergence

© Risk Reward Ltd UK. All rights reserved. Available by subscription only – not for sale or resale
I Introduction

“This man, on one hand, believes that he knows something, while not knowing (anything). On the other hand, I – equally ignorant – do not believe (that I know anything),”

– Socrates in Plato’s The Apologies

The notion of Socratic ignorance has been a ideological theme for centuries. As the notion goes; the wise man is not he who thinks he knows everything, rather he who knows that he does not know everything.

Since ancient times, this idea has formed a common thread in philosophy. Its application to the fields of economics and politics has, however, been a more recent phenomenon. As recently as 2004, in his book Fooled by Randomness, Nassim Nicholas Taleb applied the idea to financial markets. He proposed that the notion that financial institutions can both fully know and fully quantify the risks associated with their businesses is a false wisdom, an arrogant oversight that has a value destructive effect on their business models.

When, in 2007, Taleb published his now famous book, The Black Swan, the notion was expanded beyond financial markets into the seemingly
unpredictable and devastating events, which impact not only economics but the security of the nation. These occurrences he called ‘Black Swans’. Black Swans have now entered into the common parlance of big business, with risk managers busily deploying strategies to better predict and deal with the fall-out of Black Swans. The Boards of Directors of large enterprises are gradually realising not only that the risks to their business will never be fully quantified but also that, in this knowledge, they gain a competitive advantage by being better prepared than their competitors to deal with crises.

Institutions outside of the financial sphere are only just beginning to take note of Taleb’s important theory. So as Business (and especially financial institutions) begins to acknowledge the necessity of understanding Black Swan events and incorporating them (as best they can) into their business models, the UK Government has started to lag in its thinking around Black Swan risk.

Given the obvious importance to the nation of preventing national disasters, or at least mitigating their impact, what lessons can the Government take from the world of Business to address these risks and to add value to the national security strategy?

This Bow Briefing describes the ways in which Business analyses and protects itself from Black Swan events. By looking in detail at recent examples of national and international crises and getting visibility on both their effect on the nation and how better risk strategies could have helped to mitigate their effects, we argue that the Government has much to learn. In doing so, we make several specific and achievable policy proposals, which we have set out on page 6. The Government should embrace modern qualitative and quantitative methods of risk management, as it is only with robust governance structures and cutting-edge risk management solutions created by modern enterprise that the Government can begin to effectively cope with that elusive beast, the Black Swan.

II Black Swans

Sometimes, from seemingly harmless causes come harmful effects. When those effects make themselves known, it seems obvious what the cause of the effect was, that the effect was always going to happen.

According to Taleb, a Black Swan Event has three key characteristics:

(i) it occurs outside projected expectations (a fat tail to a distribution curve);

(ii) it carries extreme impact; and

(iii) it seems explainable after the fact.

Consider the following recent examples of Black Swan events with respect to these underlying characteristics.

Urban unrest (2011)

An Outlier

The independent Riots Communities and Victims Panel (UK) estimated that around 15,000 people were actively involved in the riots, which spread through England in the Summer of 2011 at alarming speed. The Government showed no sign of having predicted the riots and, as expected, the panel concluded that the causes of the riots were complex and were not about, or caused by, any single issue.

Volcanic Ash Cloud (2010)

An Outlier

When a relatively small volcano, Eyjafjallajokull (let’s call it ‘E’), erupted in Iceland in April 2010, it ejected material as high as 20,000 feet. This event demonstrated the inherent uncertainties of volcano science. Although volcanoes are far more predictable than earthquakes, each volcano is unique, with each one having its own personality, and, as such, predicting the timing and scope of their eruptions is notoriously tricky.

The Riots Communities and Victims Panel estimated that the costs to the country was in the region of half a billion pounds. Given the major impact on police resources and the wider economic ramifications, few would argue that the impact of the riots was not extreme.

Explainable after the fact

The Riots Communities and Victims Panel’s interim report looked at the August 2011 riots in the context of the English riots of 1981. The Panel noted that “it is thirty years since the publication of the Scarman report. The Panel is clear that the riots in August 2011 were very different disturbances to those in 1981. However, it is a sad fact that in some respects, the underlying challenges are strikingly similar”.

Volcano scientists are empiricists, who rely primarily on past performance to predict future activity. However, when
Black Swans Mean Business (Part 1)

it came to it, their methods, which included measuring the regularity with which E had previously erupted proved futile. Whereas the Iceland volcano produced only a small eruption at first, it seems now that the cause of the second, more serious eruption was that a vent, previously unknown to the scientists had opened beneath a glacier on the volcano and the resulting ‘soda pop’ effect proved devastating. This phenomenon had previously not been observed.

**Extreme impact**
The eruption of E had a significant impact on the civil aviation industry, causing thousands of flights to be cancelled and the economic destruction that limited transport entails. The eruption also had an impact on the RAF, which had to temporarily suspend flight training after ash deposits were found in jet engines. Indeed, the gridlock produced by the cancellation of air travel was deemed sufficiently serious by the previous Government to require a meeting of COBR to be convened to discuss remedial measures.

**Explainable after the fact**
With hindsight, the scientific community felt that the impact of the eruption on airspace could have been predicted and better prepared for. Following the event, the UN, through the International Strategy for Disaster Reduction (UNISDR), urged European Governments to integrate volcano risk as part of their air travel policies and legislation. It is interesting that now UNISDR is now working on greater coordination and interaction between decision makers and the scientific community to achieve meaningful results in this field.

**Fukushima power plant disaster, Japan (2011)**

**An Outlier**
When the Tsunami hit in March 2011, among several devastating effects, was the damage caused to a nuclear reactor in northern Japan. Being an area prone to earthquakes, the Tokyo Electric Power Co., owner and operator of the Fukushima Dai-Ichi plant, had erected sea barriers at the site to protect the nuclear reactors. The waves produced by that particular earthquake were so large that the sea barriers proved 8 metres too short to stop the resulting tsunami.

**Extreme impact**
The damage caused to the reactor in Japan resulted in the worst nuclear disaster since Chernobyl, 25 years previously. The Japan Center for Economic Research, a private think tank, has estimated the remediation costs to be in the region of $250 billion over the next 10 years. Of course, this does not take into the loss of life and injury that will ensue following the exposure of local inhabitants to massive amounts of radiation.

**Explainable after the fact**
Since Japan’s Fukushima disaster, Électricité de France (EDF), has allocated about £200 million to protect UK reactors from Black Swan events, such as a giant wave created by a collapse of an island as far away as North Africa. This is emblematic of a number of reactive measures taken by nations, including the United Kingdom, to protect themselves, post 2011 Tsunami from the human and economic cost of poor preparation.

**III The Current UK Government Approach**
The UK Government’s civil and national security risk is currently managed by the following organs of government:

(i) In the case of managing domestic emergencies, The Civil Contingencies Secretariat (CCS), established in 2004 under the Civil Contingencies Act (its executive committee, the Civil Contingencies Committee (CCC)),

(ii) In the case of protecting the country’s national security and other interests, the National Security Council (NSC), established in 2010, and

(iii) To manage emergencies, both domestic and international, ‘COBR (A)’, or Cabinet Office Briefing Room (A), which provides a forum for the CCC to meet and a focal point for the Government’s response.

For a full description of these bodies, please take a look at our recent paper, Intelligence Design: UK National Security in a Changing World. We provide below, however, a brief summary of the roles of these bodies, with particular regard to their risk management capabilities.

**Domestic Emergencies**
In recent years, the UK Government has made a good start on firming up its risk management architecture. The Government was one of the first governments in the world to create a national risk register (NRR) for domestic civil emergencies under the CCS. The NRR documents civil emergency risks over a 5-year time horizon including malicious risks (e.g., terrorism) and non-malicious risks (i.e., naturally occurring events and accidents). The National Risk Assessment (NRA) for civil contingencies is assessed annually to ensure it reflects the latest evidence and draws upon the best available evidence and advice from subject-matter experts.
The CCS Preparedness and Response Team systematically and routinely scans the short-range horizon (generally up to six months ahead) for potential or emerging civil domestic risks within this timeframe. CCS has links to departments, their agencies and other public bodies which are responsible for monitoring and managing civil emergency-related information. These channels have ensured that CCS receives timely notification of impending events, such as events to include wide-area flooding, suspected animal disease outbreaks such as Foot and Mouth Disease, and human health threats such as the swine flu pandemic.

International Emergencies

The NSC has adopted the methodology used in the development of the National Risk Register. The methodology used involves thinking around the impact of an event (based on economic consequences, casualties and social or structural factors) and the likelihood of such an event occurring over a determined timeframe.

The National Security Risk Assessment (‘NSRA’) is reviewed every two years and uses similar concepts to the NRA process described above. It involves making judgments about the relative impact of each risk, alongside an estimation of the likelihood of each risk. The NSRA process assesses all major disruptive risks to the UK’s national interest, which are of sufficient scale or impact so as to require action from the Government.

Using 5 to 20 year horizon scanning, the NSRA identifies and analyses a full range of real and potential risks, giving the greatest weight to those with the ability to cause immediate and direct harm to the UK’s territories. In general, a risk assessed as high-likelihood and high-impact would also be considered as a high priority for action. Similarly, those risks judged to be low-impact and low-likelihood would be considered lower priorities.

The management of domestic risks is overseen by the Joint Committee of National Security Strategy (JCNSS), which is made up of 22 members (12 from the Commons and 10 from the Lords). This provides a forum to challenge conventional wisdom and to hold the organs of Government to account.

COBR(A)

The primary function of COBR is to coordinate the national response to both domestic and international emergencies. In addition, the Cabinet Office engages proactively with central and local Government and other partners in preparing for such events by developing and testing response plans. The COBR mechanism is triggered by emergencies which require sustained central Government coordination and support from a number of Departments and where appropriate, the devolved administrations.

Recent Performance

Complex interdependencies in modern societies make it more likely that emergencies will require a large degree of co-ordination across Government.

“... there are also unknown unknowns – the ones we don’t know we don’t know. And if one looks throughout the history of our country and other free countries, it is [in this] category that tend to be the difficult ones.”

(Donald Rumsfeld, 2002)

The Government has made a reasonable start on this. A good example of developments to civil contingencies planning is the extensive contingency measures drawn up by the Government to prepare for extreme flooding in England: ‘Project Excessive Watermark’. This was undertaken following the Pitt review of the 2007 summer floods, a Black Swan event. The tests concluded that England and Wales has the capability to respond to severe, widespread flood emergencies.

On the other hand, the Government has not always been so proactive. Looking at the fuel protests of 2000 and 2012, the Government was completely underprepared for the former, and by the time the latter came along, only reactive measures had been taken by the Government, such as calling in the military, should the drivers of petrol tankers decide to stage a national strike. Ultimately the military was not required, and these preparations were time and resource consuming for COBR(A) and for Government Departments.

The lack of strategic focus resulted from a failure to be proactive and more robust architecture is needed to mitigate the effects of such occurrences. There is much to do, and the world of Business and, in
particular, the experiences of the financial sector, offers some useful ideas, which could lead to meaningful progress in this area.

IV Business Approaches

Recent Black Swan events such as the Financial Crisis, the BP oil spill in the Gulf of Mexico and the above-mentioned Tsunami in Japan have prompted businesses to plan for extreme events and look again at their risk architecture.

Complex businesses have often developed their own enterprise risk management frameworks to capture these emerging unknown risks. These frameworks employ forward-looking governance structures and quantitative techniques to assist in the decision-making process.

These organisations generally have good risk management practices for specific risks at ‘business unit’ level, but also have the ability to aggregate these risks across the entire organisation, sometimes applying correlation factors between risks.

There are formal and informal processes for escalating risks through the hierarchy of a business but they generally follow a “three lines of defence” approach, as described below:

- The 1st level of defence is the person who identifies the risk (whoever identifies the risk, is responsible for managing the risk);
- The 2nd level of defence is a separate risk management department, headed by a senior risk officer; and
- The 3rd level of defence is the Board of Directors (or appropriate governing body), supported by an independent audit function.

A risk crystallises if all three levels are breached.

The success of the three level defence system depends upon good management information systems, change management control procedures, strategic planning processes, and financial reporting conventions. In addition to this, most business organisations have an annual risk assessment review and material and emerging risks are subjected to extensive stress testing. Should a risk not be accounted for, a remediation plan will then be implemented to reduce the risk to the organisation.

The day-to-day analysis of risk varies in its nature across industries and jurisdictions. Some industries use probabilistic approaches such as planning for 1 in 200 year single or multiple events, while the others take a more qualitative approach. Some take a combination of both. The objective is to have the appropriate governance structure to identify these events, so that contingency plans can be initiated, if necessary, to mitigate the risk.

Most business organisations are aware of the dangers of ‘group think’ and they will actively seek expertise from outside the industry to formulate, or at least inform, their risk strategy. To promote this enterprise-wide risk management, most Boards are also aware of the importance of risk culture and the role it plays in identifying and escalating risks promptly through the chain of command.

These organisations generally have an experienced Chief Risk Officer who reports to a Board-level Risk Committee. The Risk Committee is generally made up of executive and non-executive directors, with an independent director as its Chairman. The external members, who come from various business disciplines, provide both independent external oversight and bring their own experience and expertise to bear.

Part 2: White Swans, March 2013

The author, Atula Abeyesekera, invites feedback and comments and can be contacted via JK@riskrewardlimited.com