"...An Isolated Risk of Rain"

Michael Barwise

The BBC weather forecaster this afternoon suggested the UK Midlands were subject to "... an isolated risk of rain ...." I'm still wondering what she thought she meant. There's always a risk of rain, whatever the current weather. After all, risk is the arithmetic product of probability and outcome. The rain's probability varies continuously from zero to one, and its outcome will depend on where it falls, what's going on at the time there and to some extent who cares about it. In the case of rain, outcome is usually of quite local nature, both temporally and spatially - something or someone gets wet for a while. Occasionally it can be more significant - a flood or a mudslide. So the interesting things for the listener to the weather forecast are the probability of rain in the general area and its expected severity. These are what the weather forecaster should have specified for maximum utility from the forecast. But an "isolated risk" is a strange amorphous beast. If it's the antithesis to a "socially connected risk" I'm truly sympathetic, but I can see no other semantically valid meaning. As a "forecast" it's useless.

You may be wondering by now what on earth I'm banging on about. After all, we all know what risk is - we use the term - and assess risks - all the time. But do we really know what we think we know? This is the critical factor that Donald Rumsfeld left out of his famous aphorism:

"As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know"

But most important of all are the things we're convinced of that are just plain wrong (e.g. the presence of "weapons of mass destruction").

A few months back I analysed a couple of hundred responses to an online survey on *"how do you define risk?"*. The respondents were almost entirely information security practitioners - who are generally supposed to be "risk professionals." But even these risk professionals could not agree on a common definition. Answers ranged from *"risk is the effect of uncertainty on objectives"* to *"risk is a vulnerability that has not been properly addressed"* via *"risk is a strategy"*.

Roughly a third of sampled respondents appeared to think that risk is an outcome, e.g. *"risk is the potential loss of something to you."* About half as many thought it's a probability, the most striking offering being *"the probability of an event having consequences"* - which is of course always unity unless we're in the domain of the "Hitch Hiker's Guide". Only a quarter of sampled respondents correctly recognised risk as a metric, and even some of these exhibited complete lack of understanding of basic statistical principles (and indeed, in some cases, of arithmetic), e.g. *"risk is the intersection of assets, threats, and vulnerabilities. Asset + Threat + Vulnerability = Risk."*

So 75 per cent of the "risk professionals" who responded to this survey were unaware they had no real idea what risk really is. That's not a good start. But perhaps the most worrying attribute of all the sampled definitions was universal failure to define their terms of reference or to offer any concrete guidance on how to apply them to the real world. So we were in the realm of pure philosophy, not risk management. Or maybe doing worse than that - passing on undigested snippets of received wisdom like automata without any coherent thought process taking place.

I submit that if we exhibited similar uncertainty about the meaning of "profit" we'd probably all go bust in a week or so. So my question, uncomfortable is it might seem, is "although we seem to be doing it all the time, are we really assessing risk or are we just kidding ourselves we are?" I suggest we're very often not, and I further propose that in many cases we shouldn't be trying to.

To justify this, we first have to ask ourselves what we're really trying to achieve when we perform what we believe to be a risk assessment, and then we must ask whether we are equipped to do it. If we're strictly honest with ourselves, the answers will both frequently be "I'm not quite sure".

Circulated as a white paper, April 2011