Why decompile likelihood?

Decompiling likelihood into any sub-elements is difficult so why do it? It's worth doing because the quality of risk analysis being provided to organisations in the guise of likelihood assessment is poor. A probability number on its own is often opaque to a non-risk trained business manager, and appears to make as little sense to many risk consultants. So, how do we improve the product, educate risk consultants, and provide a value likelihood service to our clients? We start by identifying the sub-elements of likelihood. There could be any number but let's concentrate here on three sub-elements: intent; capability; and vulnerability.

Intent to undertake a risk scenario is hard to discern. It's easy if the scenario has been conducted against you before or if an organisation has threatened to undertake the scenario against you. The JW Marriott Hotel in Jakarta has been attacked by terrorists on two separate occasions (2004 and 2009). Given these attacks, the hotel's risk team would be imprudent not to identify a high level of intent for terrorist organisations to attack the hotel in the future. But otherwise, you have to undertake systematic collection and analysis of information to identify actual intent. If you analysis can't confirm actual intent, you should not assume an elevated level of intent. Be honest with your client and say intent is unknown. And finally, when analysing intent, don't assume that your actions can reduce intent. You can reduce capability to undertake a scenario but intent remains and will likely be the driver for upgrading the required capability to undertake the scenario in the future.

Capability is more easily identified and assessed. It will usually revolve around modus operandi, relationships, personnel, training, finance, and past experience. Has company X undertaken hostile take overs before? Does it have the funds to successfully complete the take over? By way of example, Rio Tinto would be wise to expect BHP Billiton to launch further hostile take over attempts. Find these threads and you will tell a compelling capability story. Capability to implement a risk scenario can be undermined by addressing any vulnerabilities that your organisation exhibits. Think of capability and vulnerability as the 'tank' and 'anti-tank' conundrum; the tank improved with new armour drives the anti-tank missile manufacturer to improve the missile's lethality. The missile's new lethality forces the tank manufacturer to upgrade the tank's armour.

Vulnerability relates to our exposure to the risk scenario. If we have correctly identified the scenario and then assessed the capability of the organisation to carry out the scenario, we can easily review our current defence measures and then identify any additional mitigation we might require.

So, decompiling likelihood provides our clients with a well considered understanding of likelihood that will, when informed by consequence, realistically identify risk. It provides risk management practitioners with a much more robust methodology.