The Root Causes of Assessment Failures

Governing strategic risk is one of the most important functions a company’s board performs. Research shows that companies frequently fail to anticipate, accurately assess, and adequately adapt to existential threats to the success of their strategy and the survival of their organisation. Collectively, these failures are often termed, “risk blindness.”

In our last two briefings, we described the root causes of anticipation failures and steps that directors can take to avoid them. In this and the following briefing, we’ll examine assessment failures.

Once an existential risk to a company’s survival has been identified, the board’s assessment process should seek to answer accurately four key questions about it:

1. How large a negative impact could it have?
2. How soon before this risk develops into a dangerous threat?
3. How much time and resource would be required to design and implement an adequate response?
4. What warning indicators should we monitor?

The root causes of failure to answer these questions properly afflict individuals, groups and the entire organisation. Individuals, when assessing risks, often start with two basic errors, describing risks in terms of discrete events and assuming such discrete events are unrelated to each other.

Strategic risks tend to initially appear in the form of adverse trends (e.g. a competitor’s gradual mastery of a unique mix of capabilities); only later is the crossing of a dangerous threshold marked by a discrete event (e.g. the competitor’s introduction of a highly differentiated product). Moreover, many risks are actually interrelated, and, as we saw in the 2008 global financial crisis, these relationships tend to strengthen as outcomes worsen – cascades and contagions are very dangerous phenomena that are too often neglected.

Because many strategic risks are either unique or relatively rare, people rely on highly subjective estimates rather than traditional frequency-based statistics when assessing them, which opens up a Pandora’s Box of potential problems.
As Daniel Kahneman has observed, hindsight bias inevitably distorts people’s subjective assessments: “The illusion that we understand the past fosters overconfidence in our ability to predict the future.” Moreover, as Thomas Schelling noted over fifty years ago, “there is a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered seriously looks strange; what looks strange is thought improbable; what is improbable need not be considered seriously.”

Subjective assessments are usually based on heuristics (rules of thumb that conserve our mental energy) that create biases, including the tendency to focus on information that confirms existing views leading to overconfidence in the conclusions.

When quantitative models are used to help assess potential threats, deterministic methods are commonly employed, for example the classic spreadsheet with high, low, and most likely scenario estimates used as data, rather than more sophisticated approaches that are better suited to the exploration and quantification of uncertainty.

Last but not least, individuals, having made an initial subjective assessment fail to update it as new information becomes available, causing it to increasingly diverge from evolving reality.

Within groups, such as risk committees and boards themselves, more errors occur. Too often, subjective risk assessments are made by either one or just a few people who are all exposed to common social pressures towards optimism and overconfidence (the bane of all risk analysts is being derided as the team naysayer). Moreover, people producing risk assessments are frequently not required to make their underlying evidence and logic explicit, much less to have them systematically reviewed. It is also often the case that analysts do not all use the same time horizon when making their assessments, which is guaranteed to distort the aggregated likelihood that different threats will materialize.

A final problem here is confusion about the meaning of various words of “estimative probability” used in risk assessments. For example, unless an explicit scale is used, people inevitably attach a wide range of numerical probabilities to words such as “possible”, “likely”, and “probable” with little shared understanding of or agreement with the appropriateness of these numerical surrogates within the group.

A further source of assessment failure occurs at the organisational level. One issue is the “siloing” of information, and the tendency of
different organisational units to share only good news, which results in biased risk assessments. Another critical issue is the widespread use of “risk registers” or “heat maps” to aggregate and convey assessment results.

These two-dimensional reports usually focus only on the potential impact and likelihood that a threat will develop. Such approaches may be useful when the analysis is of the impact and likelihood of well-understood and suitably quantified operational risks. When applied to assessing strategic risks they omit the critical issue of how fast they may occur. Equally dangerous when assessing strategic risk is the substantial information loss due to the use of only three categories to assess both risk impact and likelihood (e.g., low, moderate, and high), multiplying the two ratings to obtain a final “risk index”, and then further aggregating these results by assigning green, yellow, and red colours to them.

Last but not least, too often directors fail to demand that clear early warning indicators are established for identified strategic risks, and that regular updates on their status are included in all board briefings.

When all the forces involved are considered, it is easy to see why assessment failures repeatedly occur. When a disaster strikes the common lament is “Nobody saw that coming!” Yet, too often, someone did or could have done had the assessment been effective. In our next briefing, we’ll review what companies and boards can do to improve their strategic risk assessment capabilities.