Future Failures that Lurk in Your Risk Register

By Neil Britten and Tom Coyne
Britten Coyne Partners

As a practical matter, a strategic risk is any uncertainty that is hard to quantify, impossible to transfer, and can quickly kill your company. The number and severity of these risks have substantially increased over the past twenty years, as radical improvements in information and communication technology have resulted in much higher levels of connectedness, and produced large increases in complexity, non-linearity, and the speed of change.

Based on our experience as executives, directors, and consultants, we have observed that corporate failures caused by unaddressed strategic risks almost always arise from the most neglected quadrant in a typical SWOT analysis: the one where external threats interact with internal organizational weaknesses. We divide these external threats into four categories: a company's right to operate, the size and growth of its served markets, the relative strength of its competitive advantage, and the economic viability of its business model. Organizational weaknesses include three fundamental failures: to anticipate these threats, to accurately assess their potential impact, and/or to adequately adapt to them.

A recent report from McKinsey noted that, while most "major companies have risk management processes in place to identify, assess, and respond to ongoing and emerging risks to the business…many are finding these inadequate for today's volatile and uncertain environment." A key part of many enterprise risk management processes is the (usually color coded) "risk matrix" or "risk register" which aims to list the risks facing a company and categorize the severity of the threat they pose, based on the interaction of each risk's likelihood of occurrence and the potential size of its negative impact. Many of these risk registers also note the "risk treatment" that is being applied to reduce either the likelihood of occurrence and/or the potential negative impact, as well as the "owner" of the risk in question.

Unfortunately, more than a few directors and boards are uncomfortable with this approach, sensing that it may be missing something important. In our view, these fears are not misplaced. Overreliance on a risk matrix can contribute to the three organizational weaknesses that are key root causes of company failure.

<u>Failure to Anticipate</u>

- Too many risk registers ignore strategic risks, especially those in the form of trends developing over time, rather than discrete events. Put differently, too many risk registers focus not on true uncertainties, but rather on operational and financial risks that are easy to quantify, price, and transfer to others.

- Risks associated with the successful execution of critical projects are too often also missing from the corporate risk matrix.

- Also usually missing are risks to a company that are caused by the operation of normal human biases, such as overoptimism, overconfidence, confirmation, and conformity.

- Risk registers focus on individual risks in isolation, and do not organize them into groups of risks that can materially reduce the probability of achieving strategic goals. While the "risk rating" of individual risks may each be low, their cumulative impact (which can sometimes be non-linear) may still create a substantial risk that a strategic goal will not be achieved.

Failure to Assess

- As it is often implemented, the simple "probability times impact" approach used to categorize the severity of risks facing a company has many limitations.

- The determination of different risks' probabilities and potential impact are often highly subjective, based on the views of different people, and usually not systematically reviewed for the soundness of the underlying evidence and logic.

- It is often not clear whether the estimated potential impact of a risk is before or after the application of a risk treatment.

- Due to the use of broad categories to define potential impact (e.g., "severe"), risks whose potential impact differs by an order of magnitude (10x) or more may be found in the same cell of the matrix.

- As the intelligence community has found, different people can attach very different quantitative likelihood to so-called "words of estimative probability" such as possible, likely, moderate, high, probable, etc.

- Positive and negative correlations between risks (in terms of both their probability of occurrence and potential impact) are generally not taken into account.

- When subjective assessments of broad categories of risk probability and impact are mechanically combined into a single "risk rating number" the loss of useful information is immense (e.g., is a "6" risk with a category 1 probability and category 5 potential impact really the same as a "6" risk with a category 5 probability and category 1 impact?)

- The probability that each risk will occur and its potential negative impact conditional on occurrence is assessed in isolation. There is rarely an attempt to assess how the probability, impact, and interaction between different risks would be affected by the development of different scenarios. In point of fact, different scenarios will quite likely produce very different risk profiles and aggregate strategic and financial exposures.

Failure to Adapt

- Risk treatments are too often narrowly focused either on controls and/or means to transfer some or all of the estimated financial exposure that results from the risk. Attempts to explicitly optimize the amount of exposure reduction for a given amount of spending on risk control and transfer are rare.

- Actions that could be undertaken to alter the probability that an event will occur or a trend will develop in an adverse direction are usually missing from the risk register. So too are actions to develop business options that will rise in value if an adverse outcome occurs. This is also the case for actions that would limit the potential impact of key biases, including overoptimism, overconfidence, confirmation, and conformity.

- Early warning indicators and processes that would enable early detection of adverse outcomes are often missing from risk registers.

- Too often, resiliency is addressed at the individual risk level, and only physical resilience is considered. The financial and organizational resiliency that are critical to absorbing the shock of adverse risk outcomes are usually not addressed.

- The connections between the development of the risk register, development of strategy and budgets, and the execution of critical projects and initiatives are usually either weak or non-existent. Instead, risk registers are usually viewed as a compliance and reporting tool.

As this brief critique of typical risk registers has highlighted, the unavoidable and uncomfortable truth is that the successful governance of risk can never be reduced to a simple number or a colored cell in a matrix. In point of fact, the strategic risks that pose the gravest threat to a company's survival are usually true uncertainties, whose probability of occurrence and potential impact defy reliable quantification. There is no escaping the fact that – as has been the case throughout history -- successful governance of these risks requires both strong board processes and superior director judgment.