ISTOCKPHOTO

The GlobalEthicist

Risky business

Andrea Bonime-Blanc considers why reputational risk is in a cross-cutting category of its own when an organisation is considering the hazards it might face

While every organisation (whether for profit, non-profit, governmental or academic) will face varied threats, it's important to understand how universal risks might apply to a particular business or entity.

It is safe to say that any global actor may have several or all of the following big bucket risk categories to deal with at any given time: political, operational, financial, legal, supply chain, technological, and leadership/culture.

And then there is something we loosely call "reputation risk". What is reputation risk? Is it a separate risk category to add to the list or is it another kind of threat altogether? I would argue that it is not an additional category but a different kind of cross-cutting risk – an altogether different animal that is nevertheless interconnected with the other seven categories.

Let's work our way through that statement. It is arguable that some of the seven categories have overlapping issues, and we could manage with fewer overall categories. Each of these major categories, however, is distinct and emanates from a different place. Let's define these contours and then revisit how reputation risk relates back to these categories.

Political risk. This category refers to risks emanating from the particular location, its government (whether local, provincial, state, national, federal or multinational), and the state of political and socio-political affairs in that location. Thus, political risk is greater or lesser depending on whether a country has a stable and peaceful political system where leadership turnover is predictable and non-violent and civil liberties are protected, whether there is an effective division of government branches, whether an independent judiciary exists, whether regulators exercise judgment without undue influence or conflicts, and whether there is due process.

Operational risk. This category refers to risk embedded in company operations – the overall administration and organisation of the entity, its workforce, labour and payroll management, supply chain and procurement programme, business continuity and crisis management, distribution, sales and other business development channels, joint ventures and partnerships, management of local operations, and whether it is highly decentralised or centralised.

Financial risk. This category refers to the overall financial management of the organisation as well as the internal plumbing details of an organisation's financial structure, reporting, debt and leverage, financial/contractual interrelationships, internal controls, taxation, sales and business development, financial incentives, currency exchange, hedging and derivatives, state of the national and international economy, and how transactions and other financial details are collected, reported and disclosed along the financial reporting chain.

Technology risk. This risk affects most organisations in similar ways and a few in much more dramatic ways. All organisations have experienced unrelenting waves of technology change and technology based threats (cyber-threats) over the past two decades. Companies and employees need to

Reputation risk can happen in conjunction with any other types of risk

COLUMNIST: ANDREA BONIME-BLANC

adapt quickly to new risks and opportunities. Some companies also need to be prepared for the "black swan" risk of a technological disruptor completely obliterating one or more of their services or products.

Legal risk. This big category of risks emanates from anything and everything that can be categorised as a government sanctioned law, regulation or compliance requirement in any jurisdiction anywhere. Thus it is vast and almost impossible to quantify except that all global actors have many of these issues to manage and worry about from a risk management standpoint. From corruption to fraud, from privacy to data security, from discrimination to harassment, from anti-trust to anti-money-laundering, these laws exist almost everywhere, in different shapes and forms, different regulatory and enforcement regimes and within different jurisdictions and venues.

Supply chain risk. While in the past no one would have picked supply chain risk as a separate big category of risk, it is important to do so today given the spotlight that many stakeholders are shining on this type of risk. It consists of multifaceted risks starting at the inception of a supply chain (quality and integrity of ingredients or proper vetting of third party providers), and encompassing every step along the way (quality, health, safety, environmental compliance of factories, facilities, products, locations, corruption, labour issues, fraud, acts of god), to the end product (integrity, quality, safety of product or service as advertised).

Disruption of a supply chain comes in many categories and proper risk, compliance and procurement planning for both supply chain integrity and back-up plans is essential.

Leadership/culture risk. This is a distinct category of risk for a very simple reason: leadership malfeasance (or culture/ethical failure) can have some of the most significant adverse impacts of any risk category. Think about the leadership and culture failures at Enron, WorldCom, Parmalat, Adelphi and Arthur Andersen to understand how a bad culture always trumps compliance and risk management. Indeed, good leadership and a culture of integrity while hard to measure and identify may be the best form of risk management out there.

So why, one might ask, doesn't reputation risk merit its own special category? The answer is that reputation risk can happen in conjunction with any one of the above risks if it continues unaddressed and unmitigated and persists or is repeated over time.

Here are a few examples of how each of the above specific risks can also become reputational risks (and thus have more serious, longer-term negative implications for an organisation):

- Doing business in a blacklisted nation (political).
- Ignoring local licensing and permitting requirements (operational).
- Mischaracterising earnings or expenses in financial statements (financial).
- Improperly protecting intellectual property and secure data on servers (technology).
- Permitting subversion of money-laundering controls for illicit purposes (legal).
- Condoning child or slave labour (supply chain).
- Allowing a culture of retribution and fear (leadership/culture).

When do any of the above risks become a broader and more endemic reputation risk? Reputational damage will happen when, in any of the above scenarios, additional factors are present.

First, negligent or intentional failure (or avoidance) by management, the chief executive and/or the board, to identify and acknowledge that such a major risk is serious, material or worthy of a mitigation action plan. And/or second, an inability, ineffectiveness or unwillingness of management or the board to tie the management of such serious risks back into the business plan and strategy of the organisation.

An example might include Wal-Mart's supply-chain risk which became unfortunate reality with the Rana Plaza building collapse in Bangladesh that killed more than 1,000 garment production workers. The factories in the building were in Wal-Mart's third party supply chain and had persistent and major fire safety and other building violations that were not caught or addressed effectively. Layer this disaster on top of a series of similar concerns and events happening in Wal-Mart's supply chain over a period of years before this event and the contours of an additional reputational hit begin to emerge.

An effective enterprise risk management (ERM) programme using the big picture risk categories above and drilling down to where such risks live will help an organisation to identify salient risks (through, for example, assessment and surveys), weigh the likelihood/impact of risks and help prioritise them properly for effective decision-making and action planning.

But, no matter how developed an ERM programme is, reputation risk management will not be effective if it does not include two other key components: 1) executive management and board support and deployment of mitigation action plans and 2) tying the material risks back into the business plan and strategy of the organisation.

This is how reputation risk is layered on top of the other big bucket risks – it can have a multiplier and longer-term negative or positive impact on the organisation depending on the awareness and commitment of the board of directors and the C-suite. ■

Reputation risk management will not be effective if it does not include executive management and board support

Dr Andrea Bonime-Blanc is chief executive of GEC Risk Advisory, a global governance, risk and reputation consultancy to boards and the C-suite. She is chair emeritus of the Ethics and Compliance Officer Association, a member of Ethical Corporation's editorial advisory board, a programme director at The Conference Board and a life member of the Council on Foreign Relations. @GlobalEthicist