EXECUTIVES AND RISK: WHAT YOUR TEAMS WON'T TELL YOU

Our regular risk-expert columnist **Annie Searle** on why risk managers should provide the missing link in boards' understanding and translation of risks

Annie Searle

Annie Searle is a faculty lecturer at the University of Washington's Information School, where she teaches courses she designed on operational risk, ethics, policy and law as relevant to information technology. She is also principal of Annie Searle & Associates LLC, engaged in research and consulting through the ASA Institute of Risk and Innovation

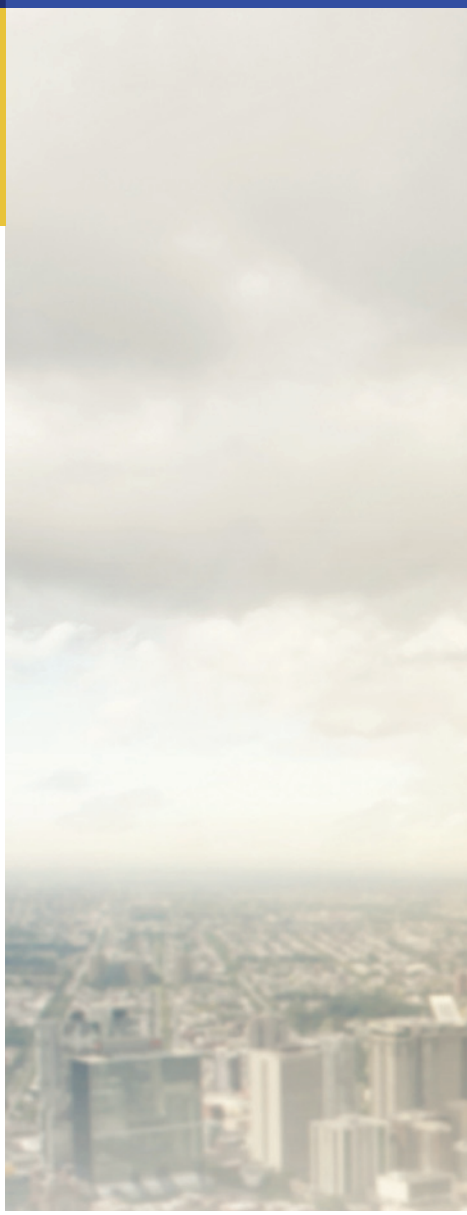
There are so many global risks that present themselves today, it is difficult to select a topic for a *Risk Universe* swan song – but first my thanks to publisher Mike Finlay and editors Victoria Tozer-Pennington and Carrie Cook for a great run over the past five years.

Operational risk management is still a relatively new discipline. Like other disciplines that have evolved in a complex technological world, the maturity of practitioners varies widely. In the past nine or so years, as companies have spun out of control, we've seen corporate managers rebrand themselves into this field or get promoted into it without necessarily understanding risk frameworks or methodologies. There is a great deal of variation in the maturity of established risk programmes inside large companies and in where such a programme is housed organisationally.

Risk management differs from audit or compliance management in that it has forward-looking, strategic, business intelligence components. It does not simply measure what is already in place with an eye to finding deficiencies. In this sense, it most closely resembles programmes like information security or business continuity, which have both forward-looking assessment and operational elements for dealing with corporate disruptions. Tools like information security's threat analysis and business continuity's business impact analysis can provide some key building blocks for an operational risk programme. Both tools rely upon a close and keen understanding of critical business processes within a company and are designed to track interdependencies and impacts.

Many firms now have risk management programmes in place, but still experience financial losses that are a direct result of failures in people, processes, systems or external events. How can executives best utilise the risk management programmes they already have in place? Or improve them?

Executives are often the last to know what might go wrong inside



their companies. The larger the company, the greater the level of complexity – and the greater the possibility that teams from audit or compliance programmes really only report what they observe at the time of the audit, or reprise what they have seen in the past. Auditors and regulators frequently have an outdated understanding of technology and/or products based upon new innovations in technology. Look how long it took regulators to understand cloud computing, which American regulators identified initially as just another kind of vendor risk. Though training for regulators has increased, it is still difficult to understand evolving technologies and practices such as high-speed trading instruments, or even how

a ransomware attack works. Compliance personnel are concerned with the strict interpretation and reporting of compliance to the law. Add to that studies that show how disaffected most employees are from their companies and what you have is an elevated level of risk that may not be auditable and may not yet constitute a compliance issue. It is not necessarily that teams don't report elevated levels of risk, so much as it is that the forms of analysis and protocols for reporting by auditors and/or regulators make it almost impossible for an executive to ask the right question of his/her team(s). So where is the information bottleneck?

Boards of directors hire chief executive officers (CEOs) who share certain leadership characteristics, around which hundreds of *Harvard Business Review* articles are written. Certainly, *experience* counts, but because of privacy protections, liability questions and complex exit agreements, recruiters for other firms are probably not made aware of issues or remediation plans that the candidate may have experienced in previous engagements. We've seen that extreme self-confidence goes a long way in the boardroom and inside the company. Most C-suite executives have made their reputations by making bold (testerical) decisions and taking a significant amount of risk. In technology firms, often the CEO is one of the founders of the company and a different set of behaviours is required for the entrepreneur than for the CEO. In some cases, a failure by a new CEO to assume the mantle of gravitas and shed testerical behaviour causes a problem in the firm's culture, particularly if there is no experienced senior management team underneath the CEO, charged with carrying out corporate governance and policy initiatives. The easiest firm to think →

Most C-suite executives have made their reputations by making bold (testerical) decisions and taking a significant amount of risk

of in this context is Uber.

If we go back to those leadership books and *Harvard Business Review* articles, we see that they are remarkably the same in the advice they offer to senior managers and to the C-suite: the CEO is asked to delegate responsibility to a senior management team and yet held accountable for gross outcomes. For both, the leader turns into a receiver and evaluator of information shared, rather than a do-er, or a hands-on shaper of the information. In the charged atmosphere of executive decision-making, where anywhere from five to fifteen consequential decisions are made daily, it is easier to accept the information reported than to question it, especially at the executive level. Bonuses in the form of stock or cash make it easier to turn a blind eye to risks that are not completely mitigated, or to control gaps that are reported blandly. If we follow the information trail as it moves from the original identification of the problem, we see that, as we go up the reporting chain, the information becomes increasingly more sanitised from manager to more senior manager; and that the information flow among the three lines of defence begins to fray as well. Not surprisingly, conduct risk is pervasive in today's corporate environment, from the front line to the executive level. Financial loss is often the story of an executive or a manager gone wrong, concealing the true impact of a problem in order to protect bonuses and jobs.

In many firms, we have three people-risk assumptions: that the board is populated with intelligent directors capable of asking hard questions of the CEO; that the CEO hire is a good fit for the company; and that the board will step in and take action if necessary. Though boards of directors may be intelligent, they can only ask hard questions if they get useful reports. (Why was the Wells Fargo board, for example, reassured on employee turnover? Did they get accurate reports with bad explanations? Or what?) If we look at the issue of CEO fit, we see that CEOs put their senior teams together primarily on the basis of their working knowledge. All too often, executives preen in their hires – and end up hiring someone they think is just like herself/himself. The risk of course is that the senior team will simply agree with the executive rather than cause a flap by raising questions.

Directly following on the heels of people risk is process risk – financial loss that stems from flawed, broken or non-existent business processes. An example might be the conversion of detailed identification of serious risk to a dashboard that shows green, yellow or red status, without attaching the detail to the dashboard for further examination. We might see a similar sanitisation upward when reports are prepared for boards of directors.

I have begun to see that perhaps the CEO does not always receive the information she/he needs to make the best decision at any given point in time

Having come from one of the largest bank failures in history, I find that I have since then revised my views on why Washington Mutual failed. Previously, I had placed the failure squarely on the shoulders of a CEO overtaken by hubris, a scholar of Jim Collins books who read and thought extensively about growth and shareholder value. It is only after having spent more time with other banks and back-tracking to detect the operational causes of financial loss that I have begun to see that perhaps the CEO does not always receive the information she/he needs to make the best decision at any given point in time. All the delegation to subordinates leads to the possibility of operational blindness. It is here that there is a real opportunity for the chief risk officer to step forward on behalf of both the board and the CEO. TRU