A Seat at the Table for Operational Risk

Annie Searle

ASA Risk Consultants
annie@anniesearle.com

ABSTRACT

What role should operational risk leaders have in the executive suite? This paper argues that, when nervous CEOs ask "What can go wrong? How can we get ahead of the curve?", they should look to their operational risk leaders. Those leaders oversee corporate and information security as well as business continuity, crisis management and disaster recovery programs inside companies. That makes them ideally qualified to take the process of crisis management, including analysis of aggregate risk across all silos -- to the CEO and then into the boardroom when the need arises, before the corporate crisis is full-blown.

Keywords

Operational risk, crisis management, pattern recognition, unknown risks, hidden risks, executive decisions.

INTRODUCTION

What if we were able to take the questions that a crisis management team asks during a disaster and apply that process across our entire business enterprise in order to answer the general question "what am I missing?" on a methodical basis, not just when we perceive that something has changed so significantly that we must address it?

Though we tend to relegate crisis management to natural disasters, security breaches or terrorist scenarios, crisis management teams inside companies are trained to work with a variety of operational risk scenarios, to ask and answer questions that allow decisions to be made on behalf of life safety (injuries, deaths, threats to health and safety), service to customers, or a threat to reputation and brand.

This paper asks what role operational risk leaders should have in the executive suite when it's not so clear that a disaster is at hand. The most recent example is of course the financial crisis, where bankers thought that market and credit risk leaders could analyze and take corrective action to manage through a narrowly scoped problem of short term profit or loss. Linkages to reputation and brand risk were not apparent, nor was the larger pattern across financial institutions, that could have pointed to the meltdown that was about to occur. Rather, it was remarked that all American banks seemed to have this problem, as if the problem was external to the institutions and was an issue of "environment." That same explanation became still another kind of justification when it was clear that all financial institutions around the world were feeling the impact and matters started to spin out of control rapidly in the spring of 2008.

This paper argues that, when nervous CEOs ask "What can go wrong? How can we get ahead of the curve?" they should include their operational risk leaders in their C-Suite deliberations. Relying simply upon color coded executive reports has not solved certain types of problems that have plagued us for the past several years, particularly in the financial marketplace – but also in other critical infrastructure sectors that also rely upon disciplines such as information and physical security, audit and compliance, internal and external fraud, and business continuity/disaster recovery. All critical infrastructure sectors need to be looking past obvious risks to those which are unknown or hidden, or where complacency has set in.

Depending upon the complexity of the event and whether or not it impacts a single company (Toyota, for example) or has a high level impact across critical infrastructure sectors (rolling power grid outages, for example), we do understand that multiple inputs are required to make decisions (White, Turoff, Van de Walle , 2007). For the purposes of this argument, "operational risk" includes the types of risk most commonly

Reviewing Statement: This paper represents work in progress, an issue for discussion, a case study, best practice or other matters of interest and has been reviewed for clarity, relevance and significance.

identified by Basel, SOX, GAAP and COSO definitions – legal and liability issues, disaster recovery and business continuity, information security, physical security, internal and external fraud, technology failures, noncompliance with regulations, inappropriate business practices and processing errors (Dickstein and Flast, 2009). I am arguing that operational risk deserves a place at the table whenever corporate wide strategic planning and risk identification is taking place, not just in the midst of a "real disaster." Operational risk leaders can help others at the table to think outside the boxes that are common to business line silos. With probing questions that span the enterprise, working from processes built to handle other types of crisis management, they can uncover unknown risks that lie outside normal risk classes; as well as hidden risks not reported by managers (Stultz, 2009).

BACKGROUND

Part of my recommendation stems from having been an operational risk executive in the banking and finance sector for nearly ten years. As head of the company's crisis management team, my focus was usually on building a program with processes that addressed potentially volatile situations that might impact shareholders or customers. It was usually easy to understand the crisis, usually, because it involved either a technology failure or a natural disaster. But the bank I worked for did not get bought because of a technology failure, or a lack of disaster recovery capacity. In fact, because we had so well documented our program and its components, we were in the process of off shoring some operational components of our technology risk management practices to help other parts of the company cut expenditures to navigate through the financial crisis. That is about as close as we got to asking "How can we get ahead of the curve on this financial meltdown?" Evaluating credit risk, hedging strategies, or offers to purchase the company was clearly not in our purview, not in the meetings we were invited to attend, nor in the strategic planning efforts we were briefed on. It was left for team of executive committee members to work behind the scenes to try to save the company. In retrospect, I can see what a crisis management/ operational risk perspective might have contributed to that discussion, which just might have been the edge needed to survive: "What is the sum total of the challenges we are facing in this moment? What else can go wrong? What is my fallback position? How can I get ahead of the curve and manage through?"

In the world of banking and finance, regulators perform "oversight" in what FDIC Commissioner Sheila Barr called a "stovepipe" fashion over the past decade, to handle the "safety and soundness" issues in financial institutions – those issues traditionally associated with market and credit risk. We are only now coming to understand just how badly our system of checks and balances, particularly in the market and credit risk arenas, failed in the past several years.

But what about operational risk, the third leg of the enterprise risk management model? What role can operational risk play going forward, as taxes, sanctions and additional forms of regulation are imposed upon critical infrastructure sectors like banking and finance? Can operational risk leaders step up at a time when the threat landscape has never been broader?

MORE THAN BANKING AND FINANCE

For in addition to the financial sector challenge to market and credit risk, other critical infrastructure sectors such as *telecommunications* have seen our security infrastructure compromised by global intruders at both the public and private sector layer. On the *information technology* sector side, we are scrambling to close holes in our systems, including those that protect intelligence and identity. Our physical security systems, in particular at airports, have shown recently not to be up to 21st century challenges (Harris, 2009). A recent study by the United States Government Accountability Office (GAO, 2009) on telecommuting assumptions that had been made indicates that there is not sufficient bandwidth to support large scale corporate remote access during an event like pandemic flu. If we look at the *public health* and *emergency services* sectors – also considered part of the nation's critical infrastructure – it's clear that budget cuts and the current economic climate have left them rusty, and vulnerable.

And as *energy* sector markets move toward greater levels of complexity, their regulatory environment is in flux, just as it is in the financial services sector. In a new white paper, Stephen Bruel from Tower Group suggests that "the capital markets comprise a complex, global interrelated system that has undergone a severe test, and is now in need of fundamental change to restore it to health" (Breul, 2009). Though most of the challenges to the global financial sector fell into the areas of market or credit risk in the past several years, we can't forget the operational risk components around business processes and internal or external fraud examples, whether the rogue trader at Societe General or Bernie Madoff himself. Information moves at the speed of light, and

mistranslation or misinterpretation leads to processing errors, another reason to examine closely the technology platforms on which this type of complexity is deployed before still more financial institutions collapse.

We are working with our international partners at a pace that seems glacial. Congressional committees investigate how disparate sophisticated intelligence agencies can fail to "connect the [intelligence] dots," and as we face a third possible wave of H1N1 at the same time climate change challenges produce earthquakes, hurricanes, fires, storms and floods. This is not a comprehensive list of current operational risks, but it does illustrate why I asked the question about stepping up our efforts in light of visible threats. We should look again at the "EPTrust" proposal made in 2004 for a means to shape a higher level of assurance around homeland security (Turoff, M. et al, 2004)

I would argue that if ever there were a need for "pattern recognition" to connect the dots, then it's to operational risk leaders that we must turn. While both market and credit risk involve statistical models and risk-based policies and procedures, it's operational risk that allows leaders to look across the enterprise and ask "What can go wrong? How can I get ahead of the curve?"

Whether government or business leaders, we need to be fast learners from all that we have absorbed in the past several months. We need to identify the missed signals and correlate disparate pieces of strategic intelligence, using our best crisis management strategies – for we are surely, without question, a set of corporate entities in a crisis.

At the heart of an operational risk framework is the concept of *continuity of operations,* the assumption that the show must go on, no matter what. Usually located within an organization's disaster recovery/business program, the tool that is used to ask "what can go wrong? How can I get ahead of the curve and have seamless availability in my operations?" is called the *Business Impact Analysis (BIA)***.** From a granular business process level, the BIA presumes that something will go wrong, and that a work-around or a response/restoration plan will be needed. At a broader level, a crisis management team operates from well-honed procedures that are based upon mitigation strategies derived from the BIA.

BIAs are a foundational tool for the identification of risk elements that include not only continuity of operations questions, but also revenue impacts, reputational, legal and brand risks. The outputs and mitigation strategies created as a result of a BIA flow into plans or playbooks, for each line of business or corporate support group (such as Legal, Communications and Human Resources departments) to utilize during events so impactful that crisis management is required.

CONCLUSION

For those of us who have managed significant natural disasters such as hurricanes or wildfires, or the fallout from terrorist events, the granularity of those critical business processes and their specific plans is essential. In other cases, we have dealt with internal fraud or the deaths of executives or the failure of a critical vendor to perform. In leading Crisis Management Teams, we have had to improvise in the midst of live events to get a clear picture that is greater than the sum of its parts: what is the cumulative amount of risk posed by this threat? Crisis management is an essential component of a strong operational risk program in any organization. Let's take its tools out of the closet and manage our businesses through the challenges that we are now facing, with better ROI. Let's give operational risk a seat at the executive table, one that is at once experienced and unique, and which complements the modeling done in the complementary worlds of market and credit risk.

REFERENCES

1. White, C., Turoff, M., Van de Walle,B. (2007) A Dynamic Delphi Process Utilizing a Modified Thurstone Scaling Method: Collaborative Judgment in Emergency Response, *Proceedings of ISCRAM 2007, 4th International Conference on Information Systems for Crisis Response and Management,* Delft, the Netherlands,, Brussels University Press.
2. Dickstein, D., Flast, R. (2009) No Excuses: A Business Process Approach to Managing Operational Risk, John Wiley and Sons, Hoboken, New Jersey.
3. Stultz, R. (2009)Six Ways Companies Mismanage Risk, *Harvard Business Review*, Boston, pp.86-94.
4. Harris, S. (2009) Too Much Information, Wall Street Journal Online, 2/17/2010, http://online.wsj.com/article/SB10001424052748704820904575055 4
5. Report to Congressional Requesters from the United States Government Accountability Office (2009) Influenza Pandemic: Key Securities Market Participants Are Making Progress, but Agencies Could Do

More to Address Potential Internet Congestion and Encourage Readiness, Washington D.C., http://www.gao.gov/new.items/d108.pdf.

6. Bruel, S. (2009) New Landscape (Or Landslide?) : Regulation's Impact on the Capital Markets and Technological Priorities. Tower Group White Paper, http://www.towergroup.com.
7. Turoff, M., Chumer, M., Starr, R., Klasher, R., Alles, M. (2004) Assuring Homeland Security: Continuous Monitoring, Control & Assurance of Emergency Preparedness, Journal of Information Theory and Application (JITTA), 6:3.
8. Nassim, T., Goldstein, D, Spitznagel, M. (2009) Six Mistakes Executives Make in Risk Management, *Harvard Business Review*, Boston, pp.78-81.

.