REPRINT

R&C risk & compliance

# CRISIS MANAGEMENT

REPRINTED FROM:

RISK & COMPLIANCE MAGAZINE

JUL-SEP 2015 ISSUE


www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine



Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com


www.riskandcompliancemagazine.com

ONE-ON-ONE INTERVIEW

# CRISIS MANAGEMENT

**Michael B. Schwartz**
Principal
KPMG
T: +1 (713) 319 2258
E: mschwartz@kpmg.com

**Michael Schwartz** is a principal in KPMG LLP's Forensic Advisory Services practice. He assists corporate and public sector clients in preventing, detecting and investigating fraud, waste, abuse and other misconduct. Mr Schwartz is a national leader for providing public sector, anti-bribery and corruption and crisis management-related Forensic services. Prior to his 13-year tenure at KPMG, Mr Schwartz had over 20 years of trial and other legal experience as an Assistant United States Attorney, in law firms and corporate legal departments. He is a frequent speaker nationally on fraud, waste and abuse, FCPA and compliance-related topics.

**RC: Could you provide a brief overview of the types of catastrophic events that may befall a business? Do you believe companies give enough thought to how these situations might impact their business?**

**Schwartz:** Catastrophic events typically occur within a compressed period and have the potential to critically impact a company's ability to achieve its mission. They frequently result in significant financial or reputational loss. Some triggers for crises relate to weather, environment, natural and man-made disasters, product safety and recall, equipment failure, data security breach, operational failures, loss of key staff, supply chain interruption, significant regulatory enforcement action, financial reporting fraud and leadership misconduct. Certainly, there has been increased awareness in recent years among larger companies that their reliance on technology, networks and software necessitates a disaster recovery response and mitigation plan, and that personally identifiable information, and commercially valuable information or intellectual property, must be protected from a data intrusion or breach. The often unmet challenge for companies is to think beyond these top-of-mind risks to answer the harder question: "Are we prepared for the unexpected?" The most difficult unexpected events are those with high-loss and low-frequency, the so-called 'black swans'. Black swans will occur, but by definition, whether or when a particular one will occur is unknowable.

**RC: What advice would you give to businesses on dealing with such an event? How important is it to have a clear communications channel and strategy when faced with a business crisis?**

**Schwartz:** Companies should organise their crisis response and management process around four phases: planning, response, recovery/restoration and remediation/resilience. While these phases sometimes follow a sequential path, it is frequently the case that response, recovery/restoration and even remediation/resilience may occur simultaneously. Crisis planning is typically a cross-functional, integrated and dynamic process in which a company establishes a steering committee, considers potential financial, legal and operating implications of a crisis, marshals critical internal and external resources and expertise to be ready to respond quickly, and develops external and internal communication plans to keep all its critical stakeholders well informed. Crisis response encompasses the execution of the crisis plan. Due to the 'fog of war' that is inevitable in a catastrophe, the response will evolve and the plans in place to manage the crisis may need to be changed in real time due to the reality of a particular crisis situation

as it unfolds. Recovery/restoration, including managing the aftermath, is the phase when the emergency response to the catastrophe is largely resolved, and during which organisations deal with legal and regulatory claims or proceedings, address ongoing financial and operational obligations, reputational fallout and other negative impacts remaining for the company. The recovery/restoration phase endeavours to re-establish, to the extent practicable, the company's business as it was conducted before the crisis, and seeks to return the company to normalcy. This phase naturally leads to the final phase of remediation/resilience, which includes reflecting on lessons learned, taking steps to prevent or mitigate the damage from future crises, and modifying plans to more effectively and efficiently address and manage future crises. Communication planning and execution are critical to effective crisis response and management. Competent decision-making requires accurate and timely information upon which to act – many well-designed and executed crisis responses have been upended by poor internal or external communications and related mechanisms for fact-finding. The customers, shareholders, employees and other company stakeholders all experience the crisis in a different way. Timely and accurate information, clearly communicated, goes a long way in assuaging those concerns. Crises that trigger regulatory scrutiny and ensuing media attention require even more accurate and timely disclosures to counter frequent speculation, rumours or even fear-mongering by some constituencies.

**"Companies should organise their crisis response and management process around four phases: planning, response, recovery/restoration and remediation/ resilience."**

*Michael B. Schwartz, KPMG*

**RC: What do you consider to be the essential elements of an effective crisis management strategy?**

**Schwartz:** Each of these phases includes many subcomponents. For example, scenario planning and simulations or drills are critical steps to be taken well in advance of an actual crisis. An effective fact-finding process and communication strategy crosses all phases. Periodic assessment of the overall crisis management plan and its components is also critical. Understanding possible infrastructure challenges, and challenging assumptions about

the availability of such basic items as electricity or access to employees or facilities, is particularly important in the natural disaster context. An effective organisational crisis management plan must deal with how key third parties' in turn manage crises given the interdependencies and intricacies of the supply chain at many locally based or multinational organisations. Finally, a crisis may be both caused by extreme financial pressures and may similarly manifest itself in the form of severe liquidity challenges, an imminent breach of financial covenants or share price plunge. An integral work step in developing an effective crisis management plan is to retain key advisers in advance. It is frequently the case that crisis communications professionals, forensic accountants, financial advisers, lawyers, cyber intrusion and information technology professionals, and other consultants will be needed on short notice, and there will be little time to make thoughtful decisions if those retention decisions are deferred.

**RC: How does enterprise risk management feed into the crisis management process?**

**Schwartz:** Enterprise risk management (ERM) is a vital risk mapping exercise that allows a company to gain insights into its common risks, and to use that knowledge to develop mitigation plans and take preventative actions. Effective ERM is instrumental in identifying the risks that may trigger a crisis at a particular company. As a result, these are the risks that need to be contemplated, prevented, planned for, responded to and recovered from through a well designed and executed crisis management process. ERM scoping does not always provide for an effective crisis management planning or solution. It is not always the case that an identified risk triggers a crisis – for example, an unlikely confluence of events or risks might trigger a crisis not otherwise foreseen. An effective fact-finding and communication approach is an essential component of an effective crisis management plan, although those efforts are not typically in scope for an enterprise risk management exercise.

**RC: How important is it to have clear communication channels and a solid IT infrastructure when faced with a black swan event? Can this help to reduce potential financial and reputational damage suffered by the business?**

**Schwartz:** Access to critical business systems and data is a key prerequisite to being able to have accurate and timely information upon which to make decisions, and to communicate to key stakeholders. Business continuity and resilience can be viewed as an essential, but sometimes overlooked, step in the routine business operations of an organisation. In the absence of effective

planning or visibility to crisis scenarios, regardless of whether third parties are involved, the move to cloud computing or outsourcing other IT functions only increases the challenge of keeping information flowing during a crisis. While a crisis is ongoing, the business needs to maintain operations to the extent practicable, and the business' assorted IT infrastructure, supply chain and distribution network need to rely upon and generate data for others to rely on. The phrase 'knowledge is power' comes to mind as an aspirational goal by which to maintain clear communication channels and a solid IT infrastructure.

**RC: Specifically, what are some of the key crisis management considerations most firms will need to give to their supply chain following a major disruptive event? And how do you distinguish between supply chain and distribution, sales and customers?**

**Schwartz:** Identifying concentrations of risk, or 'choke points', is a key crisis management consideration. Perhaps the best way to illustrate this is through a series of examples. It is sometimes the case that a single business unit of an organisation

supplies a key component relied on by the remainder of the business. Similarly, an external supplier may provide a critical component, or there may even be a supplier to the supplier who provides a key subcomponent on a sole source basis. A crisis at the company, one of its key facilities, an outsourced IT provider, or involving a key supplier, whether caused by a natural disaster, health or safety concerns, political causes, or for other reasons, could be catastrophic for the business. Understanding whether there are 'choke points' in the supply chain or an avoidable concentration of risk in a single third party or product, and planning for shortages or unavailability for an extended period, is a worthwhile exercise, not to mention locating alternative sources or even alternative components. There may be key distribution choke points in terms of both the logistics operation involved in product delivery as well as with organisations which act as wholesalers, or are responsible for a disproportionate amount of a company's sales. Similar planning for or even avoiding that sort of concentration risk is time well spent for every organisation.

**RC: To what extent can disruptor analysis help in assessing the risks associated with potential catastrophic events?**

**Schwartz:** The resources that a company can devote to ERM are necessarily limited. As a result, ERM tends to focus on high-frequency risks such as compliance with regulations, including Sarbanes-Oxley and the FCPA. However, black swan risks are often given short shrift by traditional ERM analysis. While we cannot predict a black swan, we can anticipate the type of disruption that a black swan will have on a company. Disruptor analysis is typically implemented by outside professionals who present the company's crisis managers and other responders with a hypothetical black swan, evaluate how well the company is prepared to respond and help to devise contingency plans to improve those responses.

**RC: What final piece of advice can you offer to business leaders in terms of implementing robust crisis management planning and response?**

**Schwartz:** Start now. Assess risk, scenario plan, develop plans to respond and communicate, run simulations and retain key third parties while you have time to do so. If you have already been through a crisis, update your plans and approaches and make sure you have the benefit of lessons learned. R&C


JUL-SEP 2015
www.riskandcompliancemagazine.com