



Forensic Focus

Managing a Crisis
- You Need to Have
a Plan

KPMG China





The worst part of a crisis is not having a plan to deal with the consequences that arise. Crises can come in many forms and it is imperative that those charged with governance anticipate the types of crises that could hit and how best to deal with any situation that occurs. Time is of the essence in a crisis and the approach and speed at which a plan is implemented will directly determine how well the crisis can be managed and loss of value mitigated. This paper sets out the types of crisis scenarios our clients sometimes face, how they come to be disclosed, the consequences of disclosure and the attributes of a good response plan.



What could possibly go wrong?

Below are some categories of scenarios that organisations experience that can lead to a crisis resulting in negative publicity, loss of confidence, investigations by regulators, questions from stakeholders, drop in share price, internal investigations, additional filings and communications with regulators.

- **Financial reporting fraud:** The misrepresentation of a company's financials, such as falsifying balance sheets, income statements, under/overstatement of assets, revenues and profit, or understating liabilities, expenses and losses to deceive financial statement users.
- **Asset misappropriation:** Occurs when management, employees and/or third parties embezzle property from the company. Typical high-value schemes including setting up parallel business entities and exfiltrating intellectual property such as drawings, designs, customer lists, technical and other trade secrets.
- **Bribery and corruption:** Bribery occurs when something of value, such as money or a favour, is given or received in exchange for some kind of influence or action that would not occur under normal circumstances. Corruption is a dishonest or illegal act with others, in particular with people in authority, to conduct dishonest or illegal acts in return for money or to get advantage using their power. The consequences of being implicated in bribery and/or corruption schemes can affect brand image and the ability to work on large contracts.



- **Money laundering, sanctions, terrorist financing:** Occurs when the proceeds of crime are layered in transactions to conceal the source of the funds with the purpose of "cleaning" the funds to re-enter the economy without raising the suspicion of law enforcement agencies. Sometimes violations involve trade or transactions by certain persons or organisations with countries and/or individuals sanctioned by regulation.
- **Non-financial issues/ discrepancies:** Occurs when there are deviations in non-financial matters when comparing the conduct within one's company against corporate regulations, guidelines, and ethical standards generally accepted by the public such as environmental, health and safety, sexual, racist behavior and other standards.
- **Cyber incidences:** Occurs when data, application, networks, and/or devices were accessed from unauthorised channels such as hack, Trojan horses and others.



Specific scenarios and indicators of risk

Set out below are a number of specific scenarios and indicators of risk that could give rise to a crisis:

Financial reporting fraud schemes

- Fake revenue and circular fund flows
- Non-arm's length transactions with related parties
- Capitalised or deferred expenses
- Unusual C level movement
- Dubious asset acquisitions/divestitures to and from non-arm's length parties with questionable values
- Hard to determine intangible values/amortisation schedules
- Opaque transactions with distributors or other TPI's
- Excessive prepayments
- Dual books/mixing of company/personal funds
- Inventory manipulation

Money laundering, Sanctions, Terrorist financing

- Receiving and paying funds from/to sanctioned countries, entities and/or individuals
- Opaque use of intermediaries in negotiating and conducting business for layering and integrating illicit funds
- Business transactions with high risk persons/entities/countries

Asset misappropriation

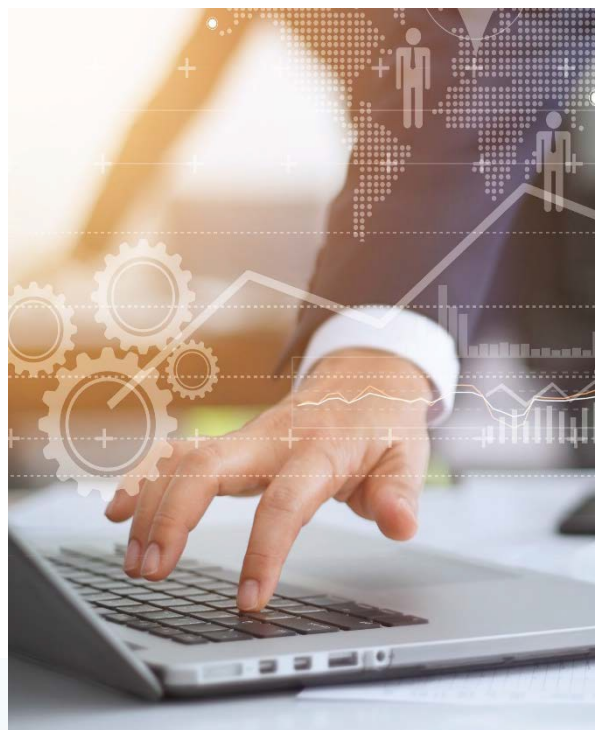
- Fake CEO fraud – urgent request to spend funds to staff's connected entities
- Business diversion
- Non-arm's length acquisitions/disposals
- False expense claims
- Payroll fraud
- Trade secret/intellectual property loss
- Deception from employees for personal gain

Bribery and Corruption

- Bribery on sales side (giving) to secure contracts
- Bribery on purchase side (receiving) - bid rigging or tendering anomalies
- Access to goods, services and/or information not properly available to the public
- Anti-competitive market and non-transparent practices

Non-financial issues/ discrepancies

- Management with obscure distance learning/life experience/doubtful qualifications
- Business operational KPI's widely different with market comparisons, significant deviation from industry norms
- Non-ethical labour practices – child/prison labour/sweat shop
- Occupational health and safety issues
- Suppliers/customers whose addresses do not match
- Employing relatives of influential people
- Undisclosed related or connected party transactions



Cyber incidences

- Insider threats
- Network intrusion
- Malicious software/malware
- Back door bypassing normal authentication or encryption
- Trojan horses
- Exfiltration



Consequences of a crisis

The consequences of a crisis can be significant and come in a number of ways, such as:

- Negative impact on a company's share price and corporate value
- Media attention on company premises
- Negative press articles and ongoing scrutiny impacting the corporate brand
- Business interruption from suppliers, customers, employers, regulators, bankers, creditors and investors
- Time and cost dealing with investigations/enquiries
- Fallout from customers, employees or others from leaked information
- Answering on-going enquiries from regulators, customers, suppliers and employees
- Need to make frequent public announcements
- Loss of public confidence



Who will disclose such problems

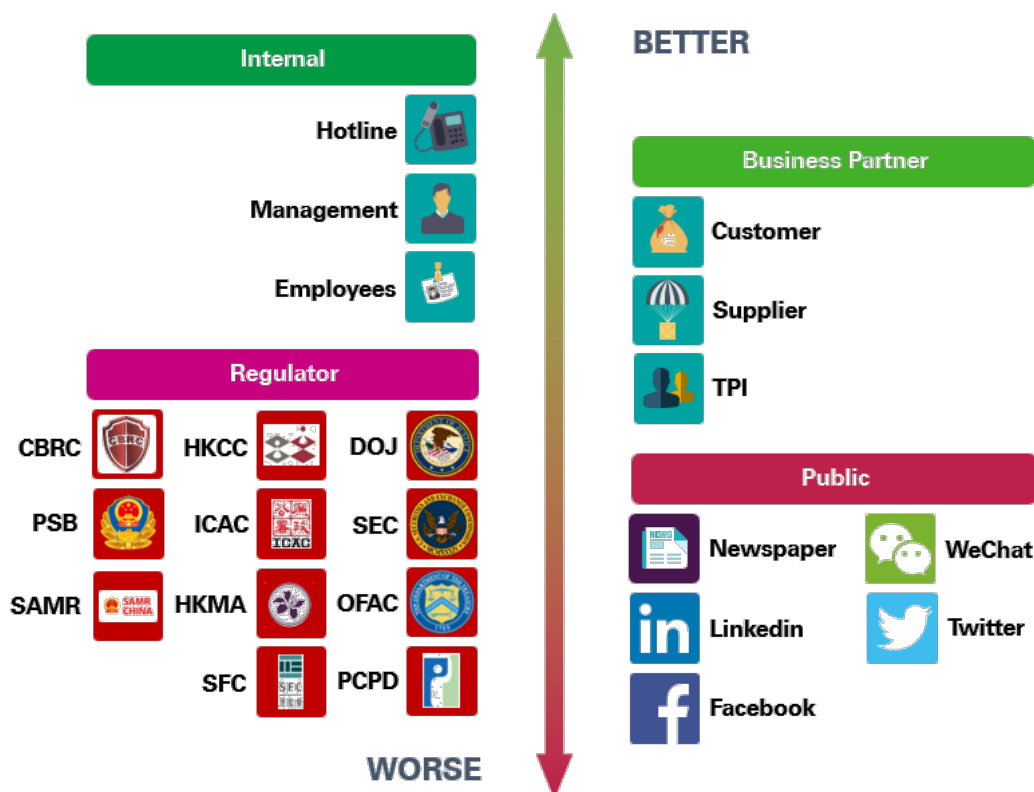
Problems can be identified and raised from a number of sources. Often, who raises the problem has a direct impact on the extent of the problem. Generally, problems that are raised and actioned internally are easier to action and manage than problems that are identified by a regulator, external parties or members of the public. The chart below illustrates the types of parties that raise such issues and provides some guidance on the likely severity of the problems at each source, all other things being equal.





How will such problems be disclosed

The extent of the crisis will also depend upon **how** problems are disclosed. For example, in the table above, you will note that an internal employee that discloses a problem directly to the regulator, perhaps motivated by a whistleblower reward scheme, or simply seeking retribution against his employer, will create far more problems than disclosing it for action internally. Most now know that regulators are far more active in monitoring for, receiving from others and acting on problems, but customers, suppliers and competitors are becoming more common as sources and recipients of complaints these days. Social media also makes it easy for any of the parties identified above to voice their concerns, anonymously, openly and instantaneously. The table below illustrates the likely severity of problems based on **how** they are disclosed, all other things being equal.



Considerations - the extent of the challenge

A crisis that is localised is far easier to contain than one that has regional or global implications. **Regional** and **global** incidents require a far more coordinated and sophisticated response plan, both within the organisation and between advisors, and must be actioned on a timely and professional basis. One of the practical challenges is how effectively and efficiently; your organisation and its international advisory team can react. Specifically, do the organisations' lawyers and forensic accountants have a good standing with regulators, and how experienced and capable are they on working with other subject matter professionals **locally, regionally** and **globally**.

Another important consideration is coordinating enquiries such that **privilege** is maintained where possible. Having teams that are familiar with these concepts at the outset is critical. Finally, it is critical to make sure that communicating the response is part and parcel of all such measures and that timely, considered and professional messages are sent to all stakeholders and/or the public as needed. Failure to **communicate** the appropriate messages can have long lasting consequences even if all the other appropriate measures are in place.

Appoint the right advisors with appropriate experience and local, regional and global reach. Make sure communications are timely appropriate and considered.



Case Study



Background

KPMG assisted a Europe based retailer that procured fashion apparel in Asia. Just before the company's Annual General Meeting, an NGO publicly "named and shamed" the company for collaborating with a business partner that allowed low occupational health and safety standards, which directly led to the fatality of a factory employee. Faced with significant global media attention, our client sought immediate independent professional assistance to ascertain what actually happened so that they could determine how to respond - both publicly on the allegation and internally as needed.



Approach

We assembled a response team, including suitable external legal counsel and a public relations firm, to quickly plan and have some people attend on site to ascertain the facts and allow the company to understand, from independent professional advisors, the issues, cause and effect and mitigation measures, and then to provide the public with an appropriate response. Our procedures included:

- Meeting with external legal counsel, internal stakeholders, internal operations personnel and public relations advisors;
- Gaining an understanding of the historical relationship with the contract manufacturer from the assessment to appointment phase, conveying of the principal's expectations around occupational health and safety policies and standards, to conducting audits on those;
- Attending the manufacturer's location at short notice and ascertain facts by reference to documents and correspondence, electronic information, telephone records and statements from management, factory and support personnel;
- Enquiries with local regulators industry bodies, transport companies, medical facilities and former staff;
- Document in detail our findings from an examination of the policies and procedures, previous compliance audits, personal accounts of events, factory and employment conditions and discussions with insurers;
- Assisting counsel to consider the implications of the findings and messaging in conjunction with the company's public relations advisors; and
- Considering the extent to which other contract manufacturers may have or could have experienced similar issues previously or going forward and recommend measures to reduce the chance of such issues recurring.



Implications

We found the facts were largely consistent with the allegations and, although uncomfortable for the company, they acknowledged the issue and a number of weaknesses with their processes and the need for immediate improvement in some areas. We also set out plans for the company to improve and monitor standards to mitigate these risks in future.

By assembling a professionally skilled response team at quick notice, the company was able to respond by noting they had commissioned an independent enquiry and would provide an update based on facts as soon as they were known. The public saw this response, and then the actual summary findings and acknowledgement of a need for improvement and confirmation that this was still a broader industry concern for similar companies; as quick, but well considered by independent professionals. Hence the public media damage was contained, and chances of recurrence mitigated.








Know your response plan

Organisations should prepare contingency plans to deal with specific and general crises. Those plans will typically require assembling the right expertise together at short notice to deal with the issues that have arisen. Ideally the teams should know each other, be on an on-call basis, and have the capacity to deal with matters that range from local to regional to international.

Typical parties assembled to respond to a crisis

The table below illustrates the types of parties typically assembled to deal with a crisis and, ideally, the groups that should seek to preserve privilege.

Response Team	Support
 Special Committee	Internal IT
 External Counsel	IT Security
 Forensic Advisors/ Accountants	Compliance
 General Counsel	Internal Audit
PR Firm	Human Resource

 Better to structure with legal privilege



Questions to consider

- Does management/the board have multiple contingency plans for a crisis?
- What types of contingencies have they planned for?
- Do you have the appropriate skills lined up on an on-call basis?
- Are those contingency plans local but global, global but local?
- Do you challenge your readiness to initiate contingency plans and navigate a crisis?



Contacts



Paul Pu

National leader
Tel: +86 (21) 2212 3780
Email: paul.pu@kpmg.com



Mark Bowra

Partner
Tel: +852 2140 2323
Email: mark.bowra@kpmg.com



Katy Wong

Partner
Tel: +852 2140 2388
Email: katy.wong@kpmg.com



Kevin Jin

Partner
Tel: +86 (21) 2212 3266
Email: kevin.y.jin@kpmg.com



Kyran McCarthy

Partner
Tel: +852 2140 2286
Email: kyran.mccarthy@kpmg.com



Rani Kamaruddin

Partner
Tel: +852 2140 2815
Email: rani.kamaruddin@kpmg.com



Mary Wong

Partner
Tel: +852 2685 7576
Email: mary.wong@kpmg.com



Cathy Zhou

Partner
Tel: +86 (21) 2212 3289
Email: c.y.zhou@kpmg.com



Dakai Liu

Partner
Tel: +86 (21) 2212 3371
Email: dakai.liu@kpmg.com



Clark Zhu

Partner
Tel: +86 (10) 8553 3650
Email: clark.zhu@kpmg.com



Melinda Phua

Director
Tel: +86 (21) 5203 1591
Email: melinda.phua@kpmg.com



Carter Zhang

Director
Tel: +86 (21) 2212 3153
Email: carter.zhang@kpmg.com

kpmg.com/socialmedia



For a list of KPMG China offices, please scan the QR code or visit our website:
<https://home.kpmg.com/cn/en/home/about/offices.html>

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG Advisory (Hong Kong) Limited, a Hong Kong limited liability company and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited ("KPMG International"), a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.