January 2016

White Paper

This white paper outlines the key principles for managing crisis and why it is a leadership issue.

Managing Crisis

Be prepared. Be transparent. Be quick.

A crisis is always a surprise and is often unique. If you'd seen it coming, you'd have avoided it. However, crisis response has many common demands, whether the situation be natural disaster, engineering failure, media fiasco or accident. To be explicit, they can, for the most part, be managed with a standard process.

You will assess the situation, make it safe, communicate, mobilize teams, make rapid decisions, solve problems, record information and make announcements. The stakes are high and you are under time pressure and public scrutiny. The price of failure is high. So even though you are surprised, you cannot extemporize. The first most important principle of Crisis Management is to have a Crisis Plan. If you are reading this because you have a crisis and no plan, you are behind the curve; it's time to call for expert help.

CEO and Board Issue

We can be confident the CEO of BP thinks crisis management is a board issue requiring personal preparation. He recently referred to the Deepwater Horizon incident as a Near Death Experience for the company. But for some, it is not clear until too late. A mismanaged crisis will expose senior management and lead to public humiliation. It damages reputations, shareholder value and can trigger losses at CEO and Board level.

Malaysian Airlines (MH) were heavily criticized after the loss of MH370 when, as is common, the CEO was expected to take public control and give news briefings under intense public scrutiny. Unlike Volkswagen (VW) whose global CEO went in days when the diesel scandal broke, the MH CEO survived to learn lessons the hard way. Sadly, MH were tested again when MH17 was shot down over the Ukraine only 4 months later. The loss of MH17 so soon after MH370 was heartbreaking, but better managed. Nonetheless the management of MH370 is what is remembered and the CEO stepped down 9 months later.

Contrast VW and MH370 with Johnson & Johnson's (J&J) handling of the Tylenol Crisis in 2002. An extortionist laced headache pills with Cyanide and seven people died. J&J went public quickly to prevent further deaths and immediately pulled the entire product line until the crisis was resolved. This is regarded a textbook case of crisis management, helped by good corporate culture. J&J remain trusted and the Tylenol brand survives today. The learning point is that CEOs and senior executives have to be ready to take personal control in a crisis. You need to ensure that preparation is done beforehand and that you, as well as your teams, are personally trained, prepared and rehearsed. Crisis management preparation and training is now simply a case of being fit for senior corporate office.

Use this white paper and the checklist on the back page to check your readiness.

Key Points

Have a Crisis Plan. Practice it.

Recognize & Declare a Crisis Quickly

Control the Situation

Have a Business Continuity Plan

Communicate Truth Rapidly

Clear Chain of Command

Preserve the Evidence

Beat the Drum

Consider a War Room

Parallel Teams

Log Assumptions

Double Check Facts and Results

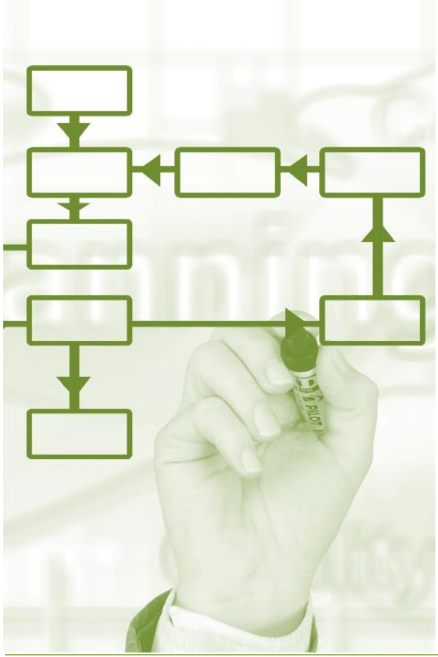
Be Cautious with Fixes

Stand Down and Tidy Up

Build Resilience through Redundancy, Diversity, and Segregation

Small Business Pointers

Businesses are now more vulnerable. Technology underpins our government, banking, personal and commercial lives. This brings great benefits, but also increases risk of crisis.



Have a Crisis Plan. Practice It.

Good practice is to define criteria and scenarios for different kinds of crisis and the first steps for each. Whilst no scenario is ever perfect, one will be close enough, and the Crisis Plan will see you through the first few hours, and put in place key people and steps to manage the issues.

I started my career emergency planning on a Nuclear Station. The Plan was very thorough. Dress rehearsals were witnessed frequently by the Nuclear Regulator. While a nuclear accident is an extreme scenario, the need for Crisis Planning is universal. Pilots train in simulators for events they hope will never happen. Hospitals rehearse their Major Incident Plans. The UK government has COBRA (named after Cabinet Office Briefing Room A). The Emergency Services rehearse for terrorist attacks in our cities.

Do normal businesses need this kind of preparedness? Yes, they do!

Businesses are now much more vulnerable to crisis than ever. Technology underpins our government, banking, personal and commercial lives. It brings great benefits, but increases risk of crisis. We cannot function if technology fails or is sabotaged. The 2012 UK Fuel crisis demonstrated again that supply lines are not just a military concern. Terrorism and cyber-attacks are prevalent. News and social media magnify issues and pour petrol on the flames.

"If you can keep your head when all about you are losing theirs and blaming it on you.
If you can trust yourself when all men doubt you, but make allowance for their doubting too."

If – Rudyard Kipling

Control the Situation

The first concern after declaring a crisis is to control the situation. If you need to control the site physically, to make it safe, for people to enter to assess the situation, to start rescue or to preserve evidence, you should call the emergency services. They are the experts in this.

You should control your teams so that they proceed in accordance with the Crisis Plan and so that you are driving the agenda. Controlling or directing the media will also be an early concern. Give priority to notifying people and mobilizing help, and to ensuring that all keep in close contact.

Cost of Poorly Managed Crisis

Volkswagen, Malaysian Airlines and BP have all faced recent crises. BP wrote off $7.5Bn for Deepwater Horizon. Volkswagen recalled 11 million vehicles and dropped 40% of its shareholder value. United Airlines grounded its fleet in 2015 because of computer failure. Arthur Andersen no longer exists. Bank IT has left customers stranded. Bank of America, Commonwealth Bank of Australia, HSBC and RBS are all recent examples.

Unmanaged crises destroy careers, companies and shareholder value. All businesses need Crisis Plans and to practice and train your people.

Recognize & Declare a Crisis Quickly

You can, even in darkest circumstances, save lives, costs and reputations by acting quickly. But if you don't recognize a crisis, you can't respond. System failures are usually clear but not all crises are obvious. VW did not respond to a university team checking their emissions data. Worse, they ducked questions from the regulator. 18 months on and the crisis has become existential for VW. Declaring a crisis requires judgement; you don't want to be late and you don't want false alarms. If Volkswagen had responded a year earlier, things could have been very different. As it is, shareholder impact is estimated at between $20 and $40 Billion.

How do you recognize the non-obvious crisis?

Firstly, ensure scenario planning is thorough. Executives should lead on crisis preparation, training, rehearsal and culture. Culture is an oft-used catch all, but here it's the standard ethics question "Would this make the front of the news, and what if it did?" Finally, you should identify explicitly who will recognize a crisis and who will declare it. Security, reception, first aiders, compliance teams, client managers, IT and PR Staff are all key front line crisis recognizers, whilst operations managers and senior executives usually declare the crisis. These people are a cross section from top to bottom of a business and in the usual course of events, they do different roles, are buried under layers of management and rarely meet. That's why you need to train all these people in the Crisis Plan and encourage direct escalation to a central point.

Have a Business Continuity Plan

A Business Continuity Plan is not a substitute for a Crisis Plan, but it is an essential component of one, A Business Continuity Plan will usually cater for specific crisis scenarios where a business needs to move locations or deal with major system failure. For example where a site has been disrupted and can no longer be used; or a major data centre fire. Large corporates will be self-insuring, they have enough sites or data centre capacity and will have a plan to move staff to a different location, and to recover critical data and systems to a new data centre. Smaller companies can arrange for staff to work from home (provided they have a mobile infrastructure) or can pay what is effectively an insurance policy to specialist companies who hold office and data centre space available in case of crisis, with these facilities being shared by many companies.

Communicate the Truth Rapidly

If you don't get the news out, someone will and you waste time correcting errors. It's almost impossible to shift a bad first impression. If you understate the issue, or hide it, you risk catastrophic loss of trust and confidence. Keep communicating with stakeholders regularly.

If a customer has a problem, don't let them find out from someone else. Equally, your boss needs to hear it from you and it is better to call the government than have them call you. Ensure your PR team is ready when journalists call. Crises have a way of making your first statement look stupid, so do it quick, don't sugar-coat it, and be clear what you don't know. In the beginning there is often a lot you don't know.

You have a few precious minutes to dig out the Crisis Plan and prepare calls and actions for clients, regulators, staff and other stakeholders. Prompt communications mobilize the organization. If people see you are in control, they will be confident and give you the most precious commodity in a crisis – time. Have an agreed notification process: who calls who, who decides. Have example messages in the Crisis Plan.

In daily life, no news is good news. In a crisis, the opposite is true. 24 hour news coverage can destroy customer confidence and company reputation in hours. After the initial message stakeholders will all need frequent contact. Issue regular updates on likely cause, impact, progress and resolution. You will need to cover conventional media, digital and social media. For a big or prolonged crisis, you will need a dedicated spokesperson or even a team.

Beat the Drum

Get people together often, face to face or on a conference call. In a small crisis, get everybody on. In a big one, it's team leaders. Use the meeting as a drum beat to accelerate the crisis cycle, to share intelligence and results, drive deliverables, escalate issues, make decisions and deploy resources.

Make the drumbeat call short and punchy. Include PR too, that way they are always briefed. My most common drumbeat is twice a day. Early morning for overnight results and to plan the day, mid-afternoon to take stock and plan the night's activities. Some organisations will move to 3 shift teams in 24 hours. But each crisis has its own heartbeat and you have to listen for it.

I recall one crisis, a banking system failure at midnight. We had hundreds of millions at stake and 6 hours before start of next working day. The drumbeat was 20 minutes: technical calls on the hour; management calls at twenty past the hour; and client calls at twenty to the hour. We fixed it at about 0450.

Consider a War Room

For bigger longer crises, there is no substitute for a War Room. Get your leaders, troubleshooters, communicators and suppliers in one place. This greatly improve pace and communication.

Crisis /'krʌɪsɪs/ noun

1) Difficult or dangerous situation needing serious attention. 2) When a difficult or important decision must be made. 3) A stage in events at which the trend of all future events, for better or for worse, is determined. 4) From the Greek word *krisis*, meaning "turning point in a disease."

> *I've seen little crises escalate and major crises averted. The difference is leadership.*

Clear Chain of Command.

I've seen little crises escalate and major crises averted. The difference is leadership. You need the right Crisis Manager – close enough to understand, senior enough to pull resources out of line, build teams and with authority to act.

Some business situations favour debate and collective decision making. In a crisis, you need a trusted leader, a chain of command and quick decisions. But you still need checks and balance. Consider appointing an Executive Sponsor, or convening the Board.

If the crisis is big, you may need two or three levels of leadership. UK Police use a Gold, Silver, Bronze concept. Gold is strategic, in overall control, a Board Member with strategic capability and authority to commit. Silver is tactical command, running the crisis operation. Bronze are team and function leaders. Identify your leaders, how they will work together and put it into your plan.

Preserve the Evidence.

You must preserve critical information - what led to crisis, its impact and how you managed it. This is a key leadership role. There may be a police or regulator investigation, a public inquiry or claims. Certainly there should be an internal lessons learned exercise. History often shows that if you don't hold the inquiry, someone else will.

Your Crisis Manager must not be compromised by the crisis and must be seen to preserve the evidence. If in any doubt, the Executive Sponsor or Board must find another Crisis Manager.

Arthur Andersen

The consequences of not preserving evidence can be horrific, they include jail and going out of business. In 2002, Arthur Andersen, a big five Accounting firm, collapsed not because they had a bad client, Enron, but because a few people in the Texas office obstructed justice by shredding the evidence. The situation should have in fact been prevented much earlier, but the local compliance leader reported to the local practice leader rather than directly to senior management and so early warning signs were missed. 85,000 job losses followed these two failures and a hallowed name disappeared into history.

Redundancy, Diversity and Segregation

Redundancy, diversity and segregation are key principles considered when building new plant and equipment. They are designed in. But these principles can also be applied to people, locations and resources to make your Crisis Plan resilient. Redundancy means if you need something in a crisis, have two, or even three of them. Multiple power supplies, back up war rooms, more than one trained crisis manager are all examples. Segregation means having critical things in different places so that they cannot be affected by the same problem. For example, keeping your backups off site. Not keeping your first aid kits together. Finally, diversity means having more than one way to do something. In a data centre context this might be having a battery bank and standby power generators. In a Crisis Plan, it might mean being able to communicate with people using different methods – radios, loudhailers etc. - in case the telephone system has also been affected.

Crisis Management is not new, just newly relevant to modern business

Market Shift and Market Collapse

These are particularly difficult forms of long-burn crisis. Market shift occurs when consumer needs change; or geography and technology render a previous market obsolete. Examples include Kodak and digital photography; Nokia and Blackberry losing to Apple; and the UK Steel Industry declining in favour of Asia. These are crises for the companies involved, but the techniques in this paper do not apply. These crises require new strategy, repositioning, major change and sometimes exit. Companies often have prolonged struggles and fall from market leadership as the products and behaviors that brought prior success are no longer effective. Apple, having essentially knocked out Nokia and Blackberry will also need to work out how to protect themselves against the *Next Big Thing* in the mobile market.

In market shift, customer needs are still satisfied and government intervention is not required, except perhaps to deal with unemployment. Market Collapse differs in that it is systemic, affecting most or all companies and customer needs are no longer met. The classic examples are banking crises (2008 Sub-Prime Mortgages), real estate and asset bubbles (1922 – 29 US Stock Market), deflation (Japan 1990s) or hyper-inflation (Weimar Republic). Some processes in this White Paper do apply to Market Collapse, but it is governments who need to step in as crisis manager of last resort. Confidence loss is widespread and recovery is usually very prolonged.

Stand Down and Tidy Up

It's important to declare a crisis over, and conduct an orderly stand down. It is now time to debrief and learn. Stand down says normal service is resuming, the press can move on; your customers and staff can relax. Others may need ongoing support. Remember to thank the teams, they will be shattered. But they also had a valuable learning experience. Check the evidence is ready. Do a lessons learned review. Conduct a root cause analysis. Use an *Ishikawa diagram* and *Human Factors Analysis* to document the crisis and how to prevent recurrence. Write up an Incident Report, then implement and monitor the preventative measures. Finally, review and update your Crisis Plan – how well did it really work? This may all seem picky, but incident learning and human factors analysis are the core reasons that air travel is so safe, and these techniques have spread widely through engineering and increasingly into services and healthcare. Standing down properly helps prevent future crises and enables you to better manage those that do occur.

Checklist

BEFORE THE CRISIS

- Scenarios prepared and are wide ranging
- Crisis plan in place and rehearsed
- Contact sheets and example messages prepared
- Notification process set up
- Staff identified and trained
- Business Continuity Plan ready
- Redundancy, diversity & segregation considered
- Separate reporting lines for compliance and crisis reporting

DURING THE CRISIS

- Crisis declared and fully notified
- Emergency & security services called if required
- Evidence preserved
- Communications under way regularly
- Crisis Manager and Exec Sponsor appointed
- Drumbeat/War Room established
- Investigation teams in place, paralleled if required
- Assumptions logged and reviewed
- Solutions tested, deployed and proven
- Stand down and debrief
- Provide post incident support if required
- Incident Report and Ishikawa complete
- Recommendations implemented
- Crisis Plan updated

About the Author

Stuart Bladen MA MBA CEng MIET has been a nuclear engineer, systems developer, and manager of Europe's largest and most critical civilian and military computer installations. He's seen a few crises, including failure of European tax systems, stalled banking systems, failures to go-live, and faulty intelligence systems. He helped to track 100,000 British Citizens missing during the Asian Tsunami. He was one of the UK Government's Red Team for Universal Credit. All these events were very different, yet he's learned that crises have a clear lifecycle and a common management approach.

Stuart can be reached at stuart@bladen.cc

Parallel Teams

Not all crises have an obvious cause and solution. When you don't know the problem, nor have a solution, you must parallel track investigation and solution teams. Simple IT crises include disk failure (no disruption with 4 hour fix) or a JCB digging up cables (it's weeks). But more complex crises are a detective story and time to fix is unclear. Separate teams should look at different angles and alternative causes or solutions. You can't afford to work serially, with one team exhausting a line of inquiry before starting the next. Investigation and solution finding is often the most challenging part of the crisis cycle, because everyone wants the answer. Confidence bleeds away easily, so keep up communication and the drumbeat.

Log Assumptions. Double Check Facts and Results

Make your teams explicitly log and check assumptions. Get an outsider to review them. Sometimes this alone solves the crisis, which may have resulted from a wrong assumption. And sometimes assumptions stop you seeing the real cause when it's staring you in the face. I recall one crisis where the team spent weeks looking for a complex network problem. It had brought a client down. They checked everything. It took an outsider to spot that the first check made on day 1 was invalid. What he knew, that the team didn't, is that the system reports had a bug, they didn't tell the truth. Once the team knew this, the problem was obvious, it was indeed the first thing they had thought of and the fix went in that night.

Be Cautious with Fixes

Good news, the team found a problem, they have a plan. You can tell everyone, but be cautious. Make sure the fix is thoroughly tested. It's only a likely fix until it's proven. Sometimes it's longer than the team expects. Sometimes one problem masks another. Sometimes side effects take longer than the original problem. Sometimes it just doesn't work. So be positive, but manage everyone's expectations. Failed fixes destroy credibility.

Small Business Pointers

Small businesses struggle to find time for crisis planning but they really need to, as their size makes them more vulnerable to business failure. Do simple plans to cover the first few steps. It will be the CEO who steps up in these cases, so make sure you delegate the day-to-day. Your surge capacity will be limited so get interim help fast if you need it. Consider outsourcing your IT to the cloud, not only cheaper and more flexible, it usually comes with resilience built in. Alternatively, consider subscribing to a business continuity service. Communication may include your bank and creditors as well as customers. Finally, speed matters even more, when your cash flow is disrupted.