# CRISIS MANAGEMENT PLANNING TIPS

## DEFINING A CRISIS SO IT DOESN'T DEFINE YOU

*By Rob Currie*

## Purpose and Summary

The purpose of this document is to explore how security professionals can define (and rate) a "crisis" and how organisations can respond appropriately and intentionally; thus, maximizing our team (or organisation's) resources most effectively.

## Defining A Crisis

### When Defining a Crisis, Context Matters

It is important to note that context plays a huge role in what one organisation might label a crisis compared to another. For example, putting out a fire for most of us would be a crisis; yet a fire department would likely see this as core business. The terms emergency, disruptive event, incident, resilience, and business continuity are increasingly common vernacular in contemporary business discussions, but is there a precise way to define?

The **British Standard 21200:2014 – Crisis management: Guidance and Good Practice**, offers a practical starting point to establishing common 'crisis language."

> *"An abnormal and unstable situation that threatens the organization's strategic objectives, reputation or viability."*

Forward-thinking organisations that adhere to modern risk management principles will attempt to anticipate and prepare for known disruptive events that affect their industry. For example, every year many businesses based in the Caribbean region prepare for tropical storm season. This notion of predictability would categorize tropical storms in the Caribbean as incidents. They occur cyclically with known mitigation measures and response mechanisms. A crisis is far more unique in nature and offers a far greater challenge to an organisation where traditional responses may not address the impact(s) of the disruptive event.

> **TIPS**
> - DEFINE WHAT WOULD CONSTITUTE A CRISIS FOR YOUR ORGANISATION.
> - RESEARCH THE IDENTIFIED RISKS FOR FREQUENCY & IMPACT TO YOUR INDUSTRY.
> - IDENTIFY THE MOST APPROPRIATE STANDARDS OR GUIDELINES FOR YOUR GEOGRAPHY.

## *How Will it Impact Us?*

Impact is another criterion for consideration. Staying with our climate theme, a Category 5 hurricane such as Maria in 2017 would clearly be a crisis. The devastating impact of the hurricane spread across the Caribbean and hampered the responses by organisations and governments. Furthermore, Hurricane Maria occurred immediately after Hurricane Irma had already ripped through the region.  The complexities generated by these two climate events place them clearly in the crisis space.

However, some disruptive events are so short lived that their impact never forces the affected organisation into crisis management mode.  Imagine a fire in the laundry area of large hotel chain that is extinguished within minutes of being noticed. Obviously, a fire in a hotel could have devastating impact, yet well trained personnel may react right away following practised emergency procedures and the incident might never evolve.  If this same incident had been poorly handled due to lack of training, it could quickly become a crisis.

## *Global Media Velocity has Killed the Ostrich Playbook!*

An organisation can also find itself in extended crisis mode by failing to recognize that an incident is impacting or has the potential to impact them. Lack of recognition can be attributed to many reasons including a lack of crisis management experience, a hope that the incident will resolve on its own, or the corporate culture of the organisation, to name a few.

One criterion for crisis that has emerged in the last 20 years is the impact of media scrutiny.  For example, in the '70s and '80s an organisation could discretely manage a situation where a senior executive was accused of unsavoury behaviour. However, the velocity of today's global media turns any behaviour linked to ethical and social issues into headline news faster than most organisations can respond. In some cases, it is the media that "alerts" an organisation that they may have an issue.  What may have been a classic HR incident can now quickly become a reputational crisis in a matter of minutes, highlighting the importance of effective crisis communication response as part of a wider crisis management program.

> **TIPS**
> • ENSURE YOUR ORGANISATION'S DEPARTMENT RESPONSIBLE FOR EXTERNAL COMMUNICATIONS IS INCLUDED IN ALL ASPECTS OF YOUR CRISIS MANAGEMENT APPROACH.
> • ORGANISATIONS SHOULD CLEARLY IDENTIFY WHO MONITORS SOCIAL MEDIA BEFORE, DURING AND AFTER A CRISIS TO AVOID "CHASING THE TRUTH" OF THE LATEST POST.
> • DEVELOP AN INTELLIGENCE STRATEGY TO MONITOR WHAT IS HAPPENING IN YOUR GEOGRAPHY AND INDUSTRY.
> • IDENTIFY THE MOST APPROPRIATE STANDARD OR GUIDELINE FOR YOUR GEOGRAPHY — EXTERNAL STAKEHOLDERS ARE KEY TO MAKING THIS WORK.

## Rating a Crisis

There is no perfect rating matrix to delineate incident from crisis. However, many organisations with mature crisis management programs use a rating scale to establish common language to describe events, as well as to determine the appropriate response levels for their Crisis Management Team (CMT). An often adopted approach is a 1 to 5 level rating matrix (see Figure 1) built into mature crisis management plans.

| Level | Description | Escalation Activity |
|---|---|---|
| 5 | • Multiple fatalities, very serious injuries or the potential for global brand and reputation to be severely impacted.<br>• A major natural catastrophe or political disruption requiring significant corporate assets. | • Escalate immediately to Corporate CMT.<br>• Resolution of the crisis will be the main effort of the entire organisation. |
| 4 | • Fatality, very serious injury or potential for brand and reputation to be severely impacted.<br>• A natural catastrophe or political disruption requiring corporate assets.<br>• Very high-profile individual involved. | • Escalate immediately to Corporate CMT |
| 3 | • A serious security event (without fatality or major injury).<br>• A disruption caused by natural or political event.<br>• Very high-profile individual near miss.<br>• Level 2 incident affecting multiple corporate locations. | • Immediately inform Regional Management<br>• Immediately inform Corporate Head of Security |
| 2 | • Security event with the potential for external exposure.<br>• Loss of >$30k, or a high-profile individual involved. | • Dealt with by local office CMT.<br>• Business as usual.<br>• Inform Corporate Head of Security and Initiate internal communications/advisory process. |
| 1 | • Security event with no external exposure. | • Dealt with on property as business as usual.<br>• Usual no requirement for Property CMT.<br>• Routine reporting to Head of Security. |

*Figure 1 - Event rating matrix*

This matrix has a sample inventory of possible events and responses to categorize the ratings as incidents or crises, or to indicate a change in severity of an issue.

- A **Level 1 incident** is a simple event that had relatively low risk and impact. These incidents are to be managed by local offices as day to day issues with no requirement to provide senior leadership a briefing or advisory.

- **Level 2 incidents** are low to medium risk but have the potential to evolve into a reputational issue. A financial loss threshold can be set to provide some guidance as it relates to asset damage or liability exposure. The threshold is arbitrary and could vary significantly depending on the industry.  This is where a more fulsome response is required, but still handled at the local office with awareness notification to corporate office. This matrix assumes Corporate Security is the steward for crisis management but could obviously be another department depending on corporate strategy.

- **Level 2 and 3** are where incidents are likely becoming to become a crisis, especially if not properly managed.  The Level 3 is still managed by the local office but there is some ongoing connection to the corporate office for advice, support and/or direction.

- **Level 4 events** are high risk and impact.  They jeopardize the viability of the organisation yet there is a high likelihood of resolution. The initial moments of the Covid19 pandemic probably saw most organisations at this level.

- **A Level 5 event** is of the same risk and impact category but has the potential to be a "brand killer," and as a result becomes the driving focus of all senior leadership.  The level 4 and 5 events are now managed by the Corporate CMT with support from the regional/local office CMTs.

This is only an example of what an organisation might use to guide their CMTs and provide common language.  It is not meant to be an "absolute" system but rather a 'scale' to allow incidents and crises to be scaled up or down.

Another dividend of having a rating system is to avoid the proverbial "5 bell fire alarm – all hands-on deck" approach to any event that is being monitored.  Such an approach is not sustainable, it ties up senior leadership for issues that could be managed by front line practitioners, and thwarts early escalation and communication of issues by front line personnel.

---

**TIPS**
- BUILD YOUR OWN EVENT RATING MATRIX.
- REMEMBER THAT CRISES CAN EVOLVE IN BOTH DIRECTIONS – REMAIN FLEXIBLE IN THOUGHT.
- PATIENCE IS KEY TO DEVELOPING A MEANINGFUL MATRIX – RE-VISIT YOUR MATRIX OFTEN AND CHALLENGE ASSUMPTIONS.
- ENCOURAGE DISCUSSIONS IN ROUTINE MEETINGS ABOUT A CRISIS OR POTENTIAL CRISES THAT HAS AFFECTED YOUR ENVIRONMENT OR INDUSTRY.
- DISCOURAGE THE MINDSET "…IT DIDN'T/WON'T HAPPEN TO US….".

*The crisis is over – back to work!*

As Winston Churchill famously stated, "Never waste a good crisis." This rings true today. As soon as a crisis has reached the end, CMTs should immediately conduct a review process. Some organisations call this an After-Action Review or hotwash. The label is inconsequential if the process maps out what happened, what worked and what did not. Capturing these observations during the review phase converts the crisis into an opportunity for the organisation IF they commit to maintaining and institutionalizing what worked and addressing highlighted gaps. This is where an organisation can truly enter an increased resilience phase by fully embracing the lessons the crisis provided.

---

**TIPS**
- FOSTER AN ENVIRONMENT OF BRUTAL HONESTY AT ALL LEVELS.
- ASSIGN SOMEONE TO EACH ACTION ITEM AFTER THE POST CRISIS REVIEW MAKING IT A PART OF THEIR PERFORMANCE MANAGEMENT.
- PRACTISE, PRACTISE, AND PRACTISE!
- IF IN DOUBT, SEEK THE ASSISTANCE OF CRISIS MANAGEMENT PROFESSIONALS TO ENABLE YOUR PROGRAM AND/OR PROVIDE AN EXTERNAL PERSPECTIVE.

---

In conclusion, what constitutes a crisis can differ greatly from one organization to another. The key to successful crisis management for any organization is to have engagement from senior leadership to establish an empowered, effective, and representative CMT. A truly empowered CMT will be able to accurately identify and establish what constitutes a crisis within the realities of a given industry or operating environment. It will also motivate the CMT to develop and leverage tools to aid in properly identifying and quantifying the potential severity of a crisis before it occurs. This in turn will motivate an organization to ingrain proactivity into the fabric of their corporate culture.

## References

- British Standard 21200:2014 - Crisis management: Guidance and Good Practice
- Deloitte - Stronger, fitter, better - Crisis Management for the resilient enterprise (2018)
- Timeline of a crisis: The #MeToo movement comes to Google (2018)
- PWC 22nd annual Global CEO Survey (2019)