

# The 10 Golden Rules of Crisis Response

Having an effective, robust crisis management strategy and plan has always been crucial for all organizations, regardless of size, type and industry. But businesses now face a much more complex and multifaceted risk landscape than ever before—including the COVID-19 pandemic, severe weather, cyber crimes and more—making it an increasingly challenging task to ensure business continuity and employee safety and safeguard assets and brand.



As such, it's imperative that organizations ensure their crisis response is as efficient and optimized as possible. **Here are 10 best practices to consider.**

## What to Do When a Crisis Strikes

- 1** **Activate your security team without delay.** If an event looks like it could turn into a crisis, get your team on standby at the earliest opportunity.
- 2** **Follow your plan.** Ensure your team follows the *crisis management plan* that you created and rehearsed for similar scenarios. The goal is to not go off course or try to recreate the wheel—when possible.
- 3** **Exert team and meeting discipline.** Hold meetings with your security team as soon as possible. Ensure meetings have clear objectives and stick to them.
- 4** **Set your strategic intent.** Articulate your goals and ensure alignment within the team. What does success look like? This should be formally established and communicated via your communications channel(s). Doing so helps guide decision making and prioritization.
- 5** **Prioritize efforts.** Not all tasks are equal. Identify the most important things you need to focus on right now. Keep in mind that primary efforts—unlike strategic intent—are likely to change because as a crisis evolves, priorities and focus will shift.
- 6** **Ensure clarity of roles and responsibilities.** If you have multiple global, regional and local security teams, it's extremely important that every team member knows what they're responsible for.
- 7** **Conduct regular post-event evaluations.** No crisis will be exactly the same. Review past incidents, tweak your response strategies and optimize your workflows for future risks. Do this often.
- 8** **Engage in scenario planning.** Identify and plan for a variety of scenarios that could occur in the future. This is how you become proactive instead of reactive when a crisis hits.
- 9** **Have the courage to make timely decisions.** The worst decision is to make no decision at all. Security and risk leaders will be required to make well-informed decisions in the absence of certainty.
- 10** **Stay true to company values.** Exemplify company values in your crisis response. For example, if you market yourself as the number one business for customer service, make sure all your crisis responses reflect that.

## 5 Common Mistakes



- 01 Inaction and/or delayed response**
- 02 Absence of clear, consistent communication**
- 03 Lack of real-time, accurate information**
- 04 Unclear goals and direction and inefficient prioritization**
- 05 Reactive approach rather than proactive**

(Source: Jonathan Hemus, Insignia Crisis Management Founder)

## Value of Real-time Information in Crisis Management

One of the most critical tools your security team needs to ensure an effective crisis response is real-time information. When a high-impact event or crisis strikes, real-time information allows you to:



Detect the earliest indications of risks—often within seconds or minutes of an occurrence



Maximize the time needed to assess risks and accelerate responses to mitigate any potential impact



Maintain real-time, comprehensive visibility and stay informed as situations unfold



Coordinate and communicate more effectively across your team and the entire organization

**Real-time alerting solutions like Dataminr Pulse can prove vital to helping organizations respond to crises with speed and confidence. By leveraging hundreds of thousands of public data sources, Pulse delivers real-time alerts that help businesses:**

- Be the first to know of potential risks
- Make well-informed, timely decisions in critical, time-sensitive situations
- Conduct post-event evaluations to improve crisis response strategies and workflows, thus enabling them to be better prepared for future incidents
- Streamline security team's communication, collaboration, response protocols and critical information flows

[LEARN MORE ABOUT DATAMINR PULSE](#)