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

get your team on standby at the earliest opportunity. Follow your plan. Ensure your team follows the *crisis* management plan that you created and rehearsed for

to recreate the wheel—when possible.

Activate your security team without delay.

If an event looks like it could turn into a crisis,

similar scenarios. The goal is to not go off course or try

Exert team and meeting discipline. Hold meetings with your security team as soon as possible. Ensure meetings have clear objectives and stick to them.

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.

Set your strategic intent. Articulate your goals

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.

Ensure clarity of roles and responsibilities.

If you have multiple global, regional and local security

No crisis will be exactly the same. Review past incidents,

you become proactive instead of reactive when a crisis hits.

Stay true to company values. Exemplify company values

in your crisis response. For example, if you market yourself

tweak your response strategies and optimize your

teams, it's extremely important that every team member knows what they're responsible for. Conduct regular post-event evaluations.

Engage in scenario planning. Identify and plan for a variety of scenarios that could occur in the future. This is how

Have the courage to make timely decisions.

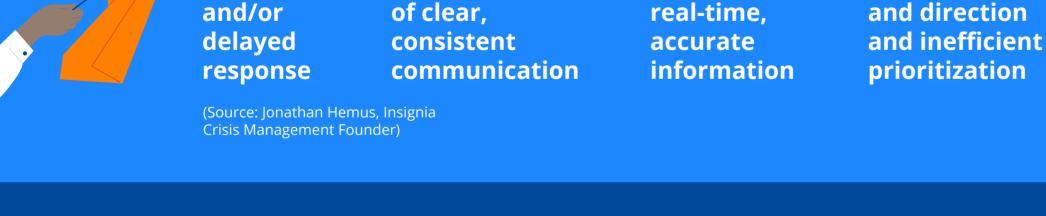
workflows for future risks. Do this often.

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.

as the number one business for customer service, make sure all your crisis responses reflect that. **5 Common Mistakes**

Lack of Inaction **Absence** of clear, real-time, and/or

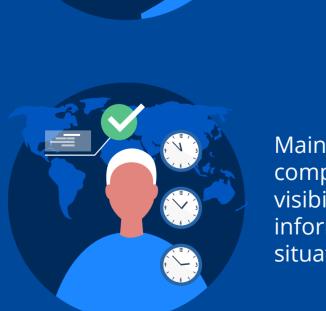
in Crisis Management



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:

Value of Real-time Information

Detect the earliest Maximize the time indications of needed to assess risks risks—often within and accelerate



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

seconds or minutes

of an occurrence



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

responses to mitigate

any potential impact

05

Reactive

approach

proactive

rather than

Unclear goals

Real-time alerting solutions like Dataminr Pulse can prove vital to helping organizations respond to crises with speed and

LEARN MORE ABOUT DATAMINR PULSE

- sources, Pulse delivers real-time alerts that help businesses:
- Be the first to know of potential risks Conduct post-event evaluations to improve crisis response strategies and workflows, thus enabling them to be better prepared for future incidents
- confidence. By leveraging hundreds of thousands of public data

Make well-informed, timely decisions

in critical, time-sensitive situations

• Streamline security team's communication, collaboration, response protocols and critical information flows