CRITICAL ELEMENTS OF CRISIS MANAGEMENT

Bob Jensen, Senior Managing Director, Strat3 LLC

Major crises happen frequently around the globe and serious incidents occur daily in nearly every city, yet many senior leaders and managers don't give crisis management the priority it requires. Whether it's wishful thinking or misinformed perception about the risks involved, nearly 66% of businesses don't have a crisis action plan according to recent surveys. Even fewer have crisis communication plans or cyber response plans. Those organizations have left themselves unprepared to handle a crisis successfully and many smaller businesses won't survive when one hits.

Some leaders think that having a Business Continuity Plan (BCP) will be "good enough" but many crises have nothing to do with a business process so a BCP won't address the issues with actions needed to respond to the crisis.

This article will look at what Crisis Management is and what the critical elements are that make up a strong crisis management effort.

Crisis Management is a key business practice area that an organization uses to plan and prepare for, respond to, and recover from any major events or threats that could harm the organization, its internal and external stakeholders, or the general public. The crisis could be sudden and provide no-notice or it could be one that builds up and is a result of a foreseen risk. It could be operational, financial, reputational, or a mixture of all three.

There are 10 critical elements of a strong crisis management practice, that I call the 10 P's:

1. **Policies**
2. **Plans**
3. **Processes**
4. **People**
5. **Partnerships**
6. **Practice**
7. **Promotion**
8. **Prediction**
9. **Prevention**
10. **Polish**

Organizations can use these 10 critical elements, and the items I've included, to do an initial assessment of where they are in their own crisis management practice and to identify what might be missing and needs to be worked on. I'll go over these elements quickly to provide a general idea of what each involves.

1. Policies: Ensure organizational policies are in place that establish a clear crisis management practice; create a Crisis Action Team and lay out roles and responsibilities; define channels of communication and alerting; mandate development of plans and strategies;and mandate appropriate training and regular exercising of those plans.
2. Plans: Ensure a Crisis Action Plan is in place that names a Crisis Action Team including who will lead efforts during a crisis and who will speak for the organization; a first 24-hours checklist; include notification procedures for employees and all key stakeholders; cover safety and legal issues; have annexes for as many key scenarios as possible based on risk assessments; include contact info and process for cooperation with local and state first responders and law enforcement. Two other important supporting plans that should be in place are a Crisis Communications Plan (that lays out key messages, holding statements, contact information for key stakeholder groups and a clear process for reviewing and approving information for public release) and a Cyber Response Plan (that covers monitoring, alerting and immediate response efforts against cyber attacks and threats since these are different from a physical situation, though they could have a physical effect).
3. Processes: Ensure both technological processes such as alert and notification systems are in place; ensure monitoring systems and processes are in place to signal up the chain when a crisis may be developing or has occurred. Are there back-up systems when primary systems fail? Are processes in place to ensure critical information is quickly transmitted to a central command post so the Crisis Action Team has the information it needs to make timely decisions on actions to take?

4. People: Ensure members of the Crisis Action Team are trained and familiar with their roles. Do all members of the organization know what to do during various types of crisis, whether natural disaster, active shooter or other issue? Are they encouraged to report up the chain when something goes wrong?
5. Partnerships: Include key suppliers and customers as part of the planning process; include contact information in annexes of the Crisis Action Plan and update regularly; partner with local law enforcement and other first responders (EMT, fire, hospital) for planning, training and exercises.
6. Practice: Ensure plans and processes, especially alert and notification processes, are tested and exercised regularly. The whole plan and individual areas can be exercised separately. A major exercise should be conducted at least once a year so key players know what the plan and processes are, so they can be ready to act when a crisis happens.
7. Promotion: Have policies, plans and processes promoted and communicated clearly to every employee and all appropriate stakeholders. Ensure information is easy to find on websites, in employee manuals, and in physical locations (e.g. at specific locations within facilities).
8. Prediction: Many situations that can potentially lead to a crisis are predictable, such as natural disasters that occur regularly (e.g. flooding in certain areas, tornadoes or winter storms during specific times of the year and earthquakes in areas prone to them), or protests that arise out of outrage or global events that may impact your organization (e.g. terrorist attacks, financial crises, pandemic). When this is the case, your crisis management plans should be activated as soon as possible and updated as additional information comes in. Also, comprehensive risk assessments for operations, physical infrastructure, financial and IT systems, and global threats help in the prediction of possible scenarios.
9. Prevention: Mitigation and prevention steps are included in your crisis management efforts such as ensuring storm shelters are available and evacuation locations are available, prior to storms hitting. Include security services, screen visitors, and hardening critical infrastructure from attacks.
10. Polish: Ensure plans, processes and results of exercises are reviewed and assessed to look for ways to improve and strengthen them on a regular basis. This is a critical step many organizations miss even if they have plans and processes in place and exercise them. The main reason to exercise them is to find gaps and areas to improve.

Working with both public and private sector organizations over the years, I found that of those who actually had a Crisis Action Plan in place, many of those plans were more than three years old and had never been reviewed or exercised. Leadership teams shouldn't be learning what's in the plan only when a crisis strikes.

Other problems included not having a Crisis Action Team established or people named to it with clear roles and responsibilities; not training teams on what needs to be done and how to do it during a crisis situation; not having the plans available in electronic form or at various locations (such as the homes of key Crisis Action Team members) since crisis can strike at any time, not just during normal business hours.

Most organizations benefit from working with outside organizations and crisis management experts to help them review and assess their crisis management practice. This is ideal for risk assessment and planning, as well as training for and exercising those plans.

Internal staff who can, and should, be a part of the development of plans and processes include risk managers, security and safety managers, operations managers, financial managers, HR and IT systems officials, legal team and corporate communicators. Of course, senior managers and top leadership should play an active role in leading crisis management plans and creating a culture of safety, prevention, preparedness, and resiliency.

While this is just a quick overview of crisis management, I hope it will provide your organization with a framework to look at where you are in your crisis management efforts. Keep reading Omnilert's Critical Mass Magazine for more useful information and best practices.

About Omnilert

At Omnilert, we believe no one should ever die or get seriously injured due to lack of timely and accurate information. Our suite of emergency notification and critical communication solutions empowers organizations to keep their people informed and their operations viable during the most challenging times. We transform the way those responsible communicate with their people to rapidly disseminate critical information, automate emergency communications, accelerate emergency response, ensure business continuity, and recover quickly from a crisis. Our people and technology, together, help ensure successful outcomes for our customers.

OMNILERT | 202 Church Street, Suite 100, Leesburg, VA 20175 | 800-256-9264 | omnilert.com