CRISIS MANAGEMENT AUDIT:

Is Your Plan Up-to-Date & Actionable?

RockDove
SOLUTIONS

Contents

Introduction

In today's fast-paced and highly-competitive business climate, most corporations have realized the importance of having a crisis management plan in place. In fact, 86 percent of organizations report that they have an emergency communications plan to prepare for crises such as fires, unplanned IT outages, natural disasters, and weather-related issues[1].

This planning work has led most board members at leading companies to feel at ease about their crisis preparedness: Three-quarters say their organization would respond effectively if an emergency struck tomorrow[2]. But when you dig deeper, it becomes clear that for many this sense of confidence is misplaced. In reality, fewer than half of companies are truly prepared for a crisis[3]—and many are relying on crisis management plans that are not up-to-date or actionable.

How would your company fare if it were struck tomorrow by one of the above crises, a data hack, an active shooter event, a social media debacle, or any of its other potential threats? How up-to-date is the content of your crisis management plan? Is it fully actionable for each member of your organization? If you are unsure, then it is already falling short.

In the first critical moments of a crisis, an up-to-date, actionable plan can minimize damage, maintain business continuity, protect your company's reputation, and in some cases, even save lives. However, an outdated, ineffective plan can cause confusion, slow response, and endanger your employees, facility, and business reputation.

The time to assess your crisis management plan is before the next crisis hits. By completing a full audit and assessing your communication response, vulnerabilities, and technology and training approach, you will be better equipped to maintain an actionable, up-to-date crisis management plan now and in the years ahead.

This eBook will guide you through an audit of your plan which is vital to assessing its effectiveness as well as help you measure your updated plan's performance and determine how to best move forward to prepare your organization for any possibility.

Does Your Current Plan Require an Audit?

You may wonder if your plan needs an audit at this point in time. To find out, think about how your current plan stacks up against best practices for your particular industry. How do corporations similar to your own handle crises? What seems to be working that you have yet to incorporate into your own plan?

Consider how your plan performs in three key areas: operational response, communications response, and coordination.

OPERATIONAL RESPONSE

These are any actions your organization will take to address a crisis in real time. Taking into account the most significant threats to your organization, do some research to discover how other corporations have handled such events. What tools did they use and how did they assign responsibilities? Did they spring into action immediately or did they lose precious minutes or hours? What was the role of external groups, such as first responders, consultants, or business partners? How might your own organization's relationships improve your operational response?

COMMUNICATIONS RESPONSE

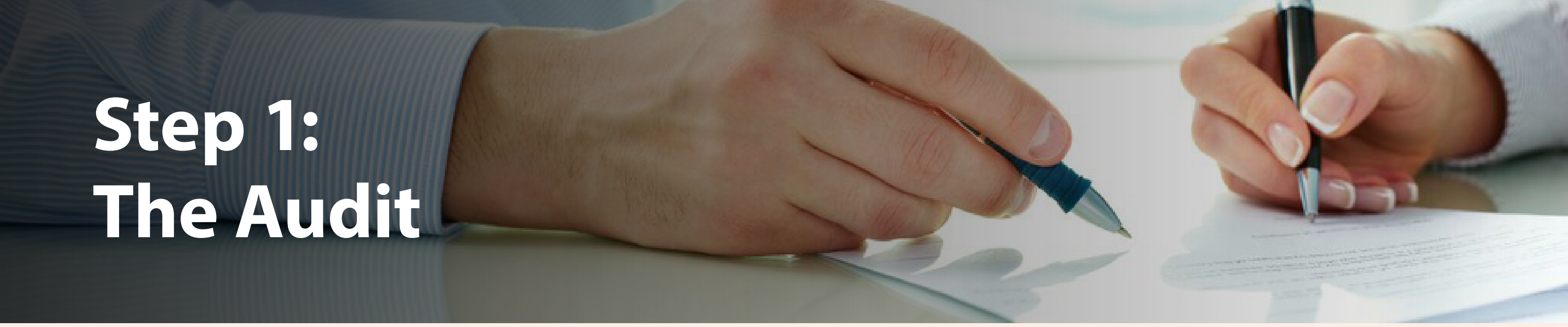
Consider the information that your organization will distribute to each stakeholder in a crisis. At a minimum, crisis plans, contact information, instructions, updates, and pre-approved messaging to communicate with the media and public should all be ready and accessible by stakeholders. Your stakeholders will likely include the executive team, employees, the media, stockholders, the public, or even family members, depending on the crisis.

During an emergency, how will key stakeholders gain details of the situation? Assess whether your plan allows for quick and easy communication with employees, both at the onset of an emergency and as it unfolds. Do all stakeholders know where to go for real-time updates and is that feasible for everyone involved? (Remember, not all employees will be at their desk or even on-site during an emergency.) Is your current plan enabling a rapid response—ideally, within an hour of the initial event?

COORDINATION

During a crisis, it is vital to coordinate messaging, the executive team, relevant stakeholders, preparing for the media, and all employees in a way that ensures they know their role, are well-informed, and are working together. Consider how you prepare your executive team for live media interviews. Who will be the point person and what will they say? What media outlet will you reach out to?

Take a careful look at the technology and other tools that your organization uses for crisis coordination, such as printed materials, websites, or information-sharing platforms. Are there newer or more advanced options in use in your industry that might help to enable faster, more effective coordination?



Step 1: The Audit

To audit your plan, you will assess its performance in four key areas:

1. Vulnerability **2. Technology** **3. Communication** **4. Training**

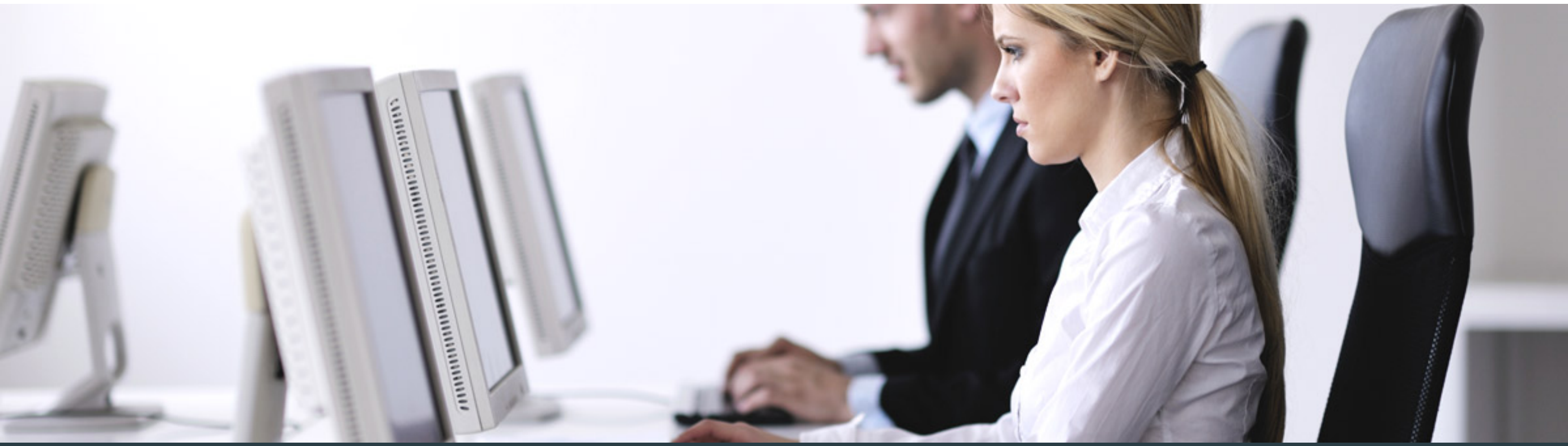
1. VULNERABILITY ASSESSMENT

First, perform a vulnerability assessment to determine current and potential areas of weakness and strength in your plan and to establish solutions. Even if your organization feels confident in its preparedness, chances are it is still vulnerable to several potential crises. Research has shown that despite having a plan in place, in reality most corporations are still vulnerable to risks such as terrorism and manmade disasters; false rumors, chemical, biological, radiological, or nuclear threats[4].

The first step in your vulnerability assessment is to take a look at any organizational liabilities that could escalate into a crisis. Ask yourself, "What is a crisis for my organization?" Consider how the various elements of your company—its people, facilities, assets, technologies, or public presence—could open the door to a crisis.

Next, review every existing document that pertains to crisis preparedness, communication, and response, looking for potential vulnerabilities. Ensure that every potential outcome is accounted for. Be sure to consider new threats that may have emerged since the documents were written. Examine changes within and outside your organization that might have an impact, such as new IT systems, hired or fired employees, company expansion, environmental conditions, and others. In addition, consider whether your plan helps your organization to achieve compliance with any local or federal codes or regulations that apply to your industry.

Be sure to focus on those crises that have impacted your particular industry. Research your industry online using search words such as crisis, complaint, and lawsuit. How did these types of crises unfold and how did the organizations involved respond? What worked and what negatively impacted the response? What lessons can you learn and apply to your own crisis plan?



2. TECHNOLOGY ASSESSMENT

Once you have detailed all your potential vulnerabilities, take a look at the various technologies and tools you use for crisis management. These may include text messaging, email, phone calls, website updates, apps, Software-as-a-Service (SaaS), file-sharing tools such as Google Drive, and other systems.

Ask yourself the following questions:

- **How are the crisis communication plans stored?**
- **How are the plans distributed?**
- **Are your distribution methods effective?**
- **When the plans are updated, how are those changes sent to stakeholders?**
- **Do you have an emergency alert notification system in place?**
- **Is there a tool for two-way communication between the critical incident response team (CIRT) and all stakeholders?**

If your answers to these questions reveal shortcomings in your devices and systems, your organization would benefit from an updated approach. Do some research on new technologies available for streamlining crisis management and communications. Today, there are systems that store plans in the cloud, making them available to every stakeholder at any time and from any location whether on or offline. These solutions also automatically notify each employee when the plans are updated, enable emergency alerts, and allow for two-way communication during a crisis.

Finally, ensure that your plans are backed up continually—and on numerous devices and systems. All methods of communication should also have a backup, particularly if cell service and internet access fail. Each stakeholder needs to be able to access the crisis plan and communicate with the CIRT at any time. Consider adding an app or SaaS platform that enables access to your documents and two-way communication without cell or internet service, which provides effective back-up in any situation.

3. COMMUNICATION ASSESSMENT

Your technology enables crisis communication, which is arguably the most important part of your overall plan. During an emergency, timelines evolve quickly. Your response can have an enormous impact on the outcome of a crisis, so it is vital to have a clear plan in place. Depending upon the threats facing your organization, clear communication can be the difference between quickly resolving a crisis and experiencing a business-changing catastrophe.

A successful crisis communication plan should include the following:

- **Clearly defined stakeholders**
- **Effective communication channels**
- **Pre-drafted, pre-approved crisis communications**

Clearly defined stakeholders.

Take a look at your current plan's stakeholders, and ask yourself whether it reflects your organization as it exists today. Consider all the people you need to communicate with during a crisis to lessen its impact and emerge on the other side unscathed. Think beyond your CIRT, employees, and customers to also include potential stakeholders such as the media, investors, the legal department, government entities, subsidiary brands, vendors, and anyone else who might be impacted by a particular threat.

Your plan should include a complete, tiered list of every stakeholder in your company, as well as their contact details and their role in an emergency. It should define stakeholder "owners": key contacts or department heads that will be responsible for providing you with any updates to the tiered stakeholder list, such as new employees or changing phone numbers.

Effective communication channels.

Are you leveraging the best methods for communicating with your stakeholders during a crisis? Research shows that the majority of crisis management plans rely upon internal emails, manual call trees, and crisis telephone lines for distributing important information during an emergency. About 50 percent of organizations use emergency communication software and/or website announcements for reaching stakeholders. Most are using some combination of the above to ensure that information reaches its target[5].

Consider the technology and tools used by your organization. Do they suit the way your stakeholders operate on a day-to-day basis—whether they are at their desks, moving throughout the facility, or out in the field? What are the best ways to reach all stakeholders—not just those who happen to be at their workstation when a crisis strikes?
It is also vital to ensure that your communication channels are robust enough to work as reliably as possible in an emergency.

Determine whether physical systems—including phone lines, websites, and email servers—could handle an uptick in traffic during a crisis. If you use a "ghost" website to serve as a central information clearinghouse for stakeholders to visit during an emergency, be sure it loads quickly and reliably.

Finally, consider how you plan to communicate with stakeholders in the event the internet and cellular phone networks fail. Remember, no single communications method is 100 percent reliable. Multiple paths of communication ensure a higher success rate—in some cases, nearly 80 percent higher[6]. Do you have a plan for multiple paths of communication to ensure successful delivery of information and response?

Pre-drafted, pre-approved crisis communications.

For most large organizations, it is helpful to have approved crisis communications plans for each threat scenario ahead of time. This saves valuable time during an emergency, enabling staff to focus on other important tasks.

Many companies write out a full draft of the communications or create a template that can be tailored to each specific crisis situation. You should have drafts (or templates) written for each potential threat scenario. For example, many organizations have text for employee announcements, social media notifications, text messages, and press releases on hand that they use in the event of an emergency. Most drafts include information such what crisis occurred, how the organization has responded, what steps will be taken in the coming hours, and any other relevant details.

If you have crisis communications written, be sure they are pre-approved. Again, this will save valuable time during an emergency and enable a faster, more organized communications response.

4. TRAINING ASSESSMENT

Finally, consider how your organization trains its stakeholders for crisis management and response. During the stress of an emergency, your people need to already know what to do and have the ability to quickly and easily reference relevant information. Currently, does your entire team know where each crisis plan is housed, as well as how to access it and what their responsibilities entail? Do you hold regular practice drills?

Also consider media training for members of your CIRT and executive team. Do you have spokespeople established for each crisis scenario? During an emergency, time is of the essence and you need to know that each member of the team can step up and confidently brief the media when necessary.

Finally, consider back-up resources. How will your organization adapt if a key stakeholder is on vacation during a crisis? Where will they go if a designated meet-up point is compromised?

You should have a backup plan for each of the following:

- **Emergency contacts for the CIRT and each department.**
- **Primary places to do business and/or emergency meeting points.**
- **Employees who perform critical duties in the plan and during normal operation.**
- **If your organization is relatively small, it is important to cross-train so that each critical role has a back-up.**

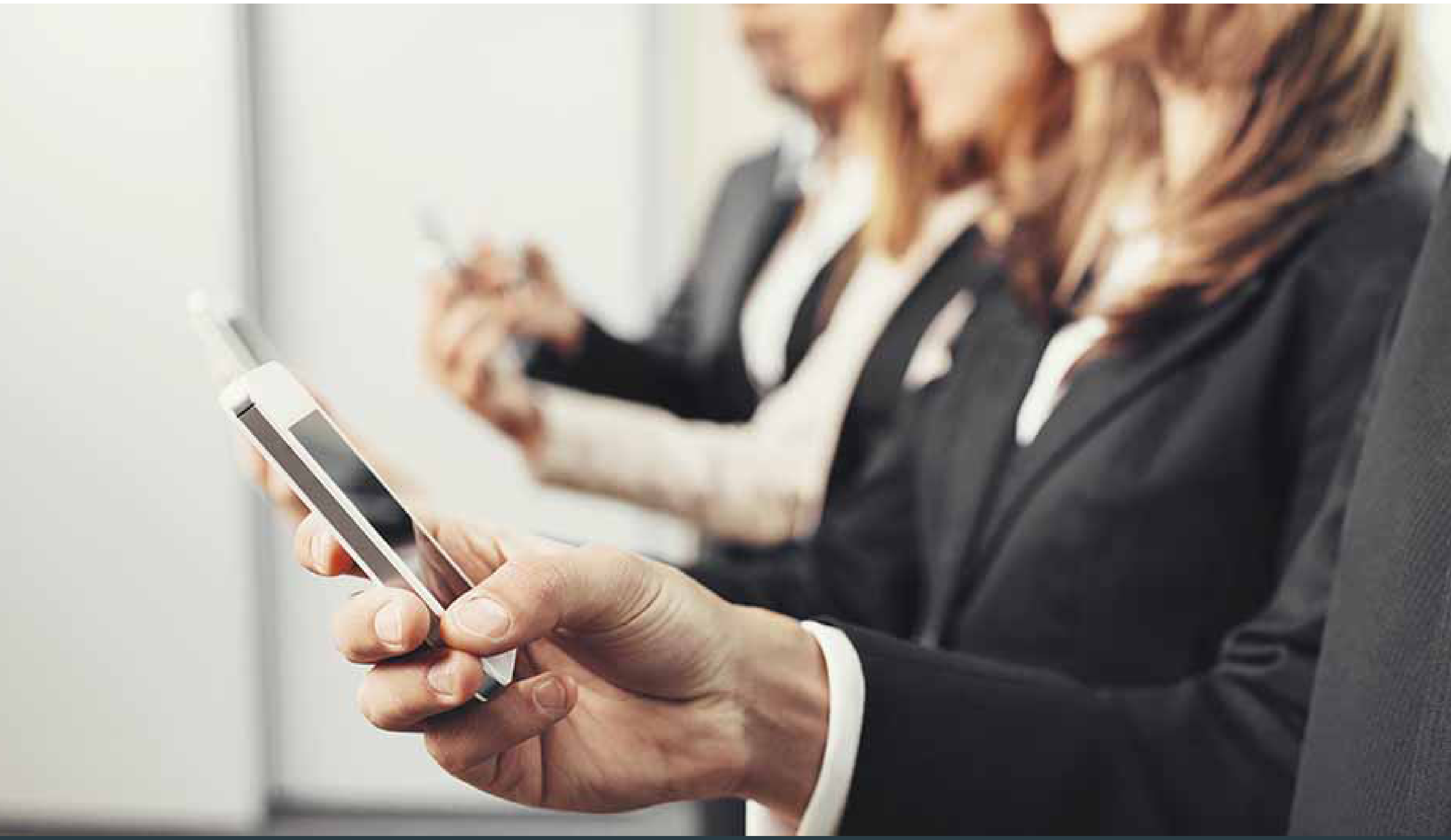
Step 2: Implement Changes

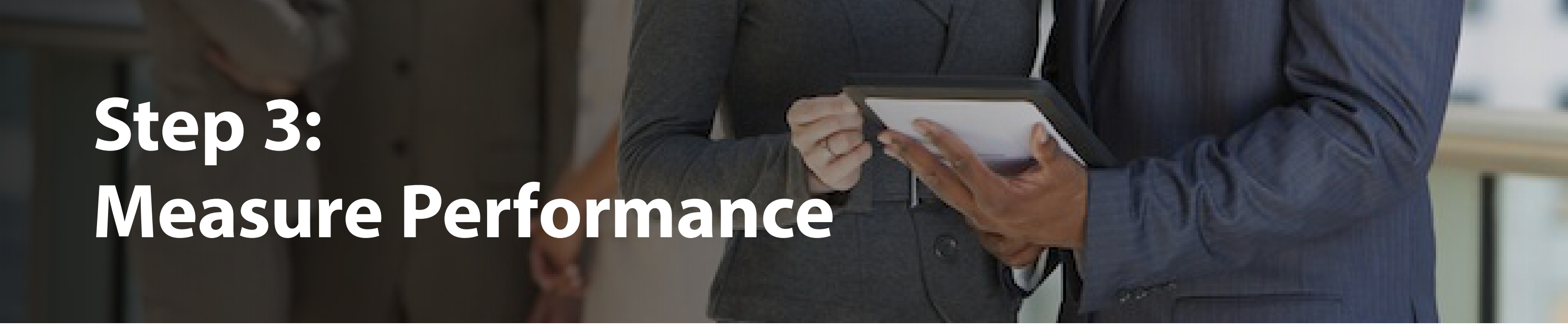
Once you have completed a full audit of your plan, consider any gaps or limitations that you discovered, and then implement updates and changes that will optimize your crisis response. This might include planning for new vulnerabilities that you have discovered or that have recently emerged; upgrading technology systems or adding multi-path communication, updating your stakeholders and drafting crisis communications, and optimizing your approach to training.

As you update the plan, get input from relevant executives as well as employees at each level of the organization. Ask them about potential vulnerabilities to ensure that you see the organization from multiple perspectives. You may uncover vulnerabilities that you had not considered in the past. For example, you might ask department heads the following:

- What IT tools does your team use for their daily tasks?
- How is sensitive information handled in your department?
- How do managers ensure that employees in the field are following the correct safety procedures?

Take what you have learned and update your plan accordingly.





Step 3: Measure Performance

Once the new plan is drafted, set aside time to run through the updated documents to measure their performance. As you conduct your tabletop exercise, assess its performance using the following questionnaire based on a worksheet developed by the Harvard Business School[7]:

CRISIS PLANNING	POOR	ADEQUATE	EXCELLENT
Does the plan account for all potential threat scenarios?	○	○	○
Does it include a flexible set of response modules?	○	○	○
Do the response modules effectively match our threat scenarios?	○	○	○
Does the plan enable immediate action from the CIRT?	○	○	○
Does it have a clear path for returning to normal operations?	○	○	○
CRISIS ORGANIZATION	**POOR**	**ADEQUATE**	**EXCELLENT**
Does the plan include a clear chain of command?	○	○	○
Does it include stakeholder responsibilities for each scenario, and is each one aware of his/her role?	○	○	○
Does each responsibility include a back-up person?	○	○	○
Does the plan use effective communication channels?	○	○	○
Does each communication channel have a back-up?	○	○	○
ORGANIZATIONAL LEARNING	**POOR**	**ADEQUATE**	**EXCELLENT**
Does our team conduct regular rehearsals?	○	○	○
Do we conduct effective post-crisis reviews?	○	○	○
Is the plan updated regularly with details such as new vulnerabilities, communication protocol, stakeholders, contact information, etc.?	○	○	○
When the plan is updated, are all stakeholders notified?	○	○	○

Once your plan meets these criteria, it is up-to-date and actionable. Make sure it is available to all stakeholders through an easily accessible platform and revisit it regularly.

Step 4: Move Forward

Following the audit of your plan, it is important to stay vigilant so that your organization is always prepared for a crisis. There are two relatively simple ways to stay on top of your plan: research continually and regroup often.

Research should become a natural part of your daily responsibilities. Collect data continually so that you are always aware of potential threats to your organization. Look to the internet and social media to be aware of the threats facing your business—and your industry.

You also need to be aware of how your organization is being portrayed in the media and on websites. Create social media streams and Google alerts for your company's name as well as relevant hashtags, industry keywords, and competitors. Ensure that you or someone within your department continually checks these resources and flags things like negative articles, threatening comments, or news of a developing crisis.

Finally, regroup often. Only 25 percent of organizations hold regularly scheduled exercises to prepare for a crisis[8] and yet employee knowledge can mean the difference between success and failure. Partner with HR to host regular refresher training sessions to ensure that employees know how to react in a crisis.

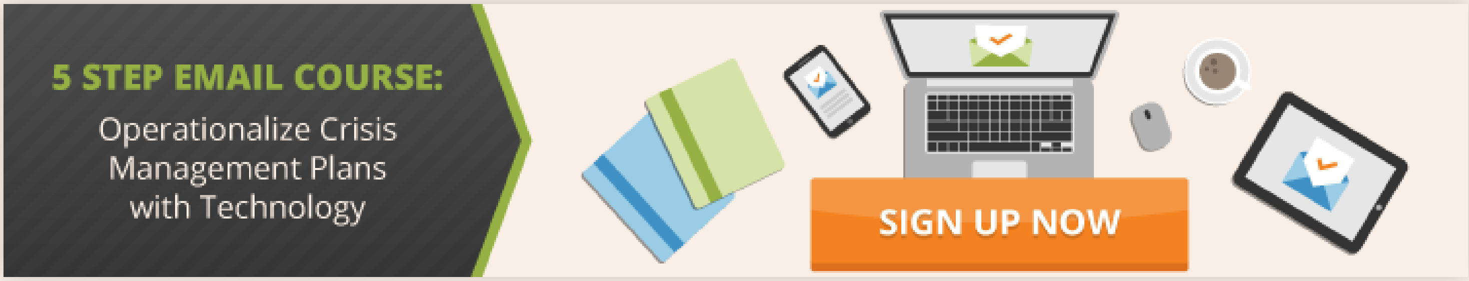
Continually analyze and test the plan, adapting it to new circumstances. It is surprisingly easy to outgrow a crisis plan so always look for vulnerabilities and gaps as your organization grows and changes. Perform your own self audits from time to time and meet at least a few times a year with the CIRT to revisit the plan in its entirety.

Conclusion

A crisis management plan should be a living document updated throughout the year in order to ensure that your organization is prepared for crises that could strike at any moment. It should also be highly actionable, enabling each stakeholder to gain quick and easy access to vital crisis information at any time and from any location.

Today's mobile technology is enabling organizations to create crisis management plans that are always up-to-date and actionable, putting information into the hands of the people who need it at precisely the moment of crisis. Using mobile apps and SaaS platforms, companies are improving access to their plans as well as empowering employees with vital features such as two-way communication, GPS mapping, and emergency alerts. With plans stored in the cloud, information can be instantly updated for all stakeholders as needed.

Crisis management can be a challenging, time-consuming task. However, when armed with an effective plan and the right technology, you can be prepared for anything that might come your way and turn a potentially devastating event into a positive effect on your organization's reputation.



Resources

[1] p.1, Alcantara, Patrick. “Emergency Communications Report 2015.” Business Continuity Institute. November 2015. Web. Accessed 4 March 2016. www.bcifiles.com/BCIEmergencyCommunicationsReport2015.pdf

[2] p.1, “A Crisis of Confidence.” Deloitte Touche Tohmatsu Ltd. 2016. Web. Accessed 4 March 2016. www2.deloitte.com/global/en/pages/risk/articles/a-crisis-of-confidence.html

[3] p.1, Deloitte, “A Crisis of Confidence.”

[4] p.3, Deloitte, “A Crisis of Confidence.”

[5] p.6, Alcantara.

[6] p.6, “Business Continuity Institute Webinar: Trends in Emergency Communications.”

[7] p.10, Watkins, Michael. “Your Crisis Response Plan: The 10 Effective Elements.” Working Knowledge. Harvard Business School. 30 Sept. 2002. Online. Accessed 9 March 2016. http://hbswk.hbs.edu/item/your-crisis-response-plan-the-ten-effective-elements.

[8] p.11, Alcantara, “Emergency Communications Report 2015.”

RockDove
SOLUTIONS

SHARE THIS EBOOK

f 🐦 in G+ ✉

www.rockdovesolutions.com