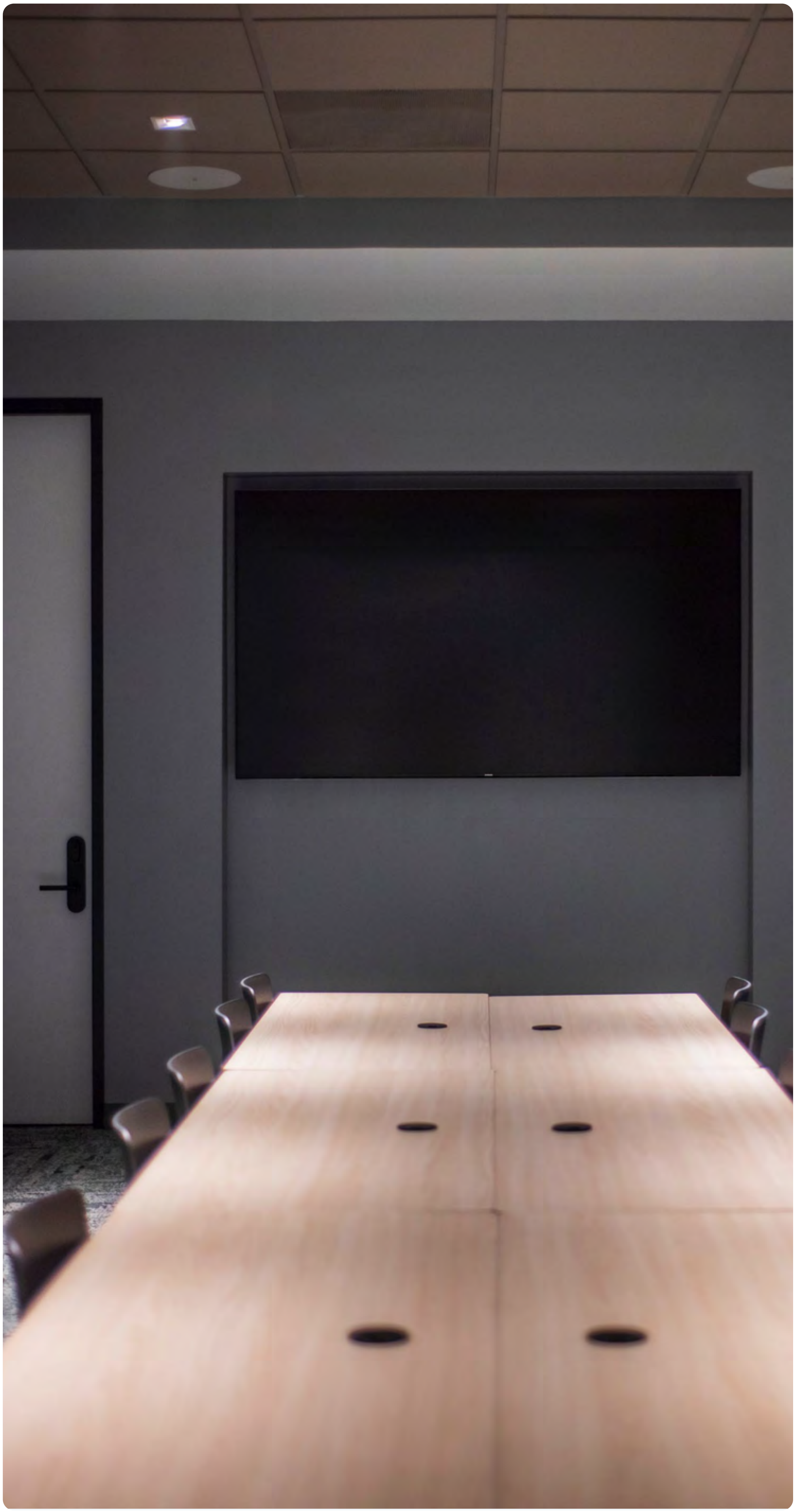
KEY STEPS TO BUILDING A CRISIS PLAN

RockDove Solutions

It Is Time to Build a Crisis Plan



In this increasingly uncertain world, many organizations which have never had a crisis preparedness plan, or only have an out-dated one that would be of no help when faced by a real threat, are seriously considering making an investment in the 'insurance policy' of a state-of-the-art issue, crisis and emergency response plan.

According to one 2020 study, only 62% of organizations have a crisis plan and very few of those companies ever update the plans or test them.

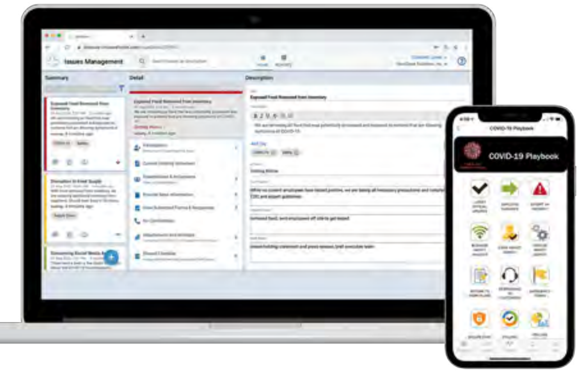
If you, or your company's leadership, require more data to be convinced it is time to build a crisis plan, then here are 22 supporting statistics.

To help get you started, we have identified the four key steps in building a modern, state-of-the-art issue and crisis management plan.

STEP ONE:
Approach for Writing, Publishing & Accessing the Plan

Why would you be thinking about where the plan would be stored, accessed, and activated even before you have written a word?

Simply, where the plan is stored and accessed will have a material impact on HOW you write it.



PLAN PUBLISHING OPTIONS:

Here are the main options.

PAPER-BASED PLAN IN A BINDER

Strengths: Paper-based plans are trusted and familiar and avoid teams having to learn any new technology, which can be a barrier to implementation. Also, there is no limit to the amount of detail and content that can be added.

Weaknesses: Huge binders are difficult to deploy in the moment of crisis as they are often not immediately accessible. Also, the amount of detail makes them hard to use in an emergency, forcing the crisis team to manage the situation ad-hoc, reinventing processes which had been laid out in the plan long before the crisis struck.

SHARE DRIVES/SMART STICKS

Strengths: These solutions at least solve the problem of quickly accessing the plan content at the moment of threat. Most people can link to their company file shares even if they are working remotely. It is also technology with which most people are comfortable.

Weaknesses: Team members have no way of knowing if they have the most up-to-date content. Also, share drives and smart sticks do nothing to help the team communicate and collaborate. For that, the team has to rely on email and chat apps, which are not secure or very efficient.

CRISIS MANAGEMENT PLATFORMS

Strengths: The best practice approach is to have the plan stored and accessed via issue and crisis management platform, such as RockDove's In Case of Crisis 365. Crisis management platforms allow easy and quick activation of the crisis response, with the team working from up to date content no matter where they are or when the threat unfolds. They also offer tools tools to help the team work collaboratively and turn plan content into actions.

Weaknesses: For some people it creates trepidation about learning a new application. It helps a great deal to have the team trained and practiced on the use of the platform ahead of any actual crisis.

TIPS FOR WRITING A PLAN

Whatever your choice of how the content will be published and accessed, there are general best practice tips about writing a crisis plan.

◆ DON'T MAKE THE PLAN TOO LONG!

There's an understandable desire on behalf of crisis plan authors to cover every eventuality, every detail of what might happen. Resist that temptation.

In the moment when a real crisis emerges, when the problem is being inflamed and spread by social media and the team is scrambling to get a response in place, there is no time to sort through pages and pages of a crisis manual.

What you are looking for is crisp, clear and unambiguous protocols, guidelines and resources – all readable and usable quickly and available on the click of smartphone icon.

◆ CHECKLISTS AND FORMS ARE EASIER TO USE THAN PAGES OF NARRATIVE

Again, there is neither the time nor the appetite among crisis team members to spend time to search the content of a plan, content of a plan.

No matter how good the thinking, dense pages of text are not helpful when the moment of truth arrives.

What you really need are:

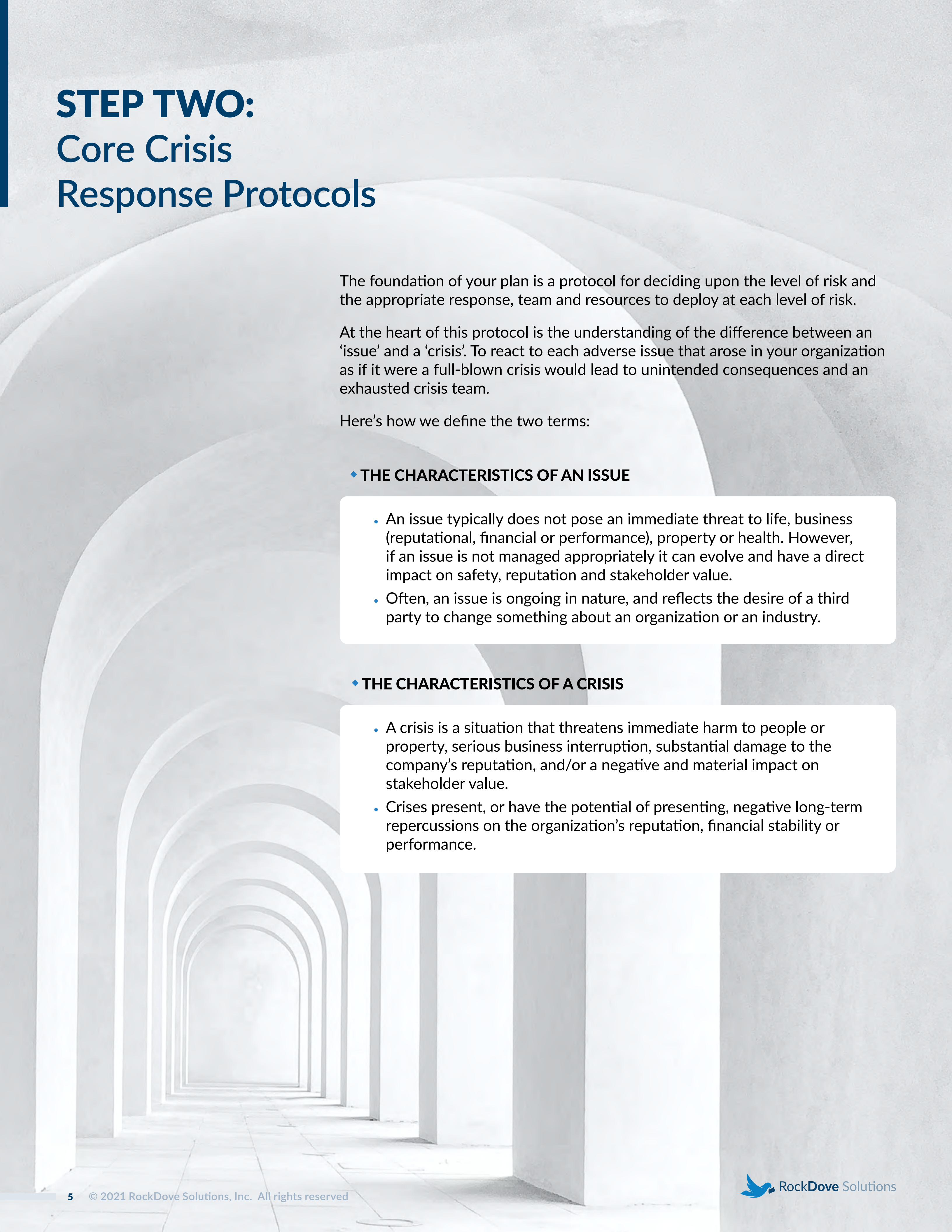
- Action steps and guidelines in checklists.
- Forms which are designed to make it easy to share information.
- Clear, bullet-pointed protocols on who to get involved and at which point in the crisis.
- Third-party resources identified and listed.

◆ NOT EVERYONE NEEDS ACCESS TO ALL THE PLAN MATERIALS

If you do embrace the best practice of having your crisis plan accessible and activated via your desktop or your mobile device, then other steps in making your plans actionable become possible.

For instance, many people on the team could have the ability to report an incident – think about ushers at a concert, managers at a restaurant chain, hotel employees or field representatives.

However, only the crisis team and senior management, who are trained and prepared to handle the response, have access to the tools, resources and protocols to manage the crisis.



STEP TWO: Core Crisis Response Protocols

The foundation of your plan is a protocol for deciding upon the level of risk and the appropriate response, team and resources to deploy at each level of risk.

At the heart of this protocol is the understanding of the difference between an 'issue' and a 'crisis'. To react to each adverse issue that arose in your organization as if it were a full-blown crisis would lead to unintended consequences and an exhausted crisis team.

Here's how we define the two terms:

◆ THE CHARACTERISTICS OF AN ISSUE

- An issue typically does not pose an immediate threat to life, business (reputational, financial or performance), property or health. However, if an issue is not managed appropriately it can evolve and have a direct impact on safety, reputation and stakeholder value.
- Often, an issue is ongoing in nature, and reflects the desire of a third party to change something about an organization or an industry.

◆ THE CHARACTERISTICS OF A CRISIS

- A crisis is a situation that threatens immediate harm to people or property, serious business interruption, substantial damage to the company's reputation, and/or a negative and material impact on stakeholder value.
- Crises present, or have the potential of presenting, negative long-term repercussions on the organization's reputation, financial stability or performance.

Therefore, when you are creating a protocol to respond to threats, a sound starting point is to create three levels of threat - the two lower levels being issues of varying degrees of seriousness and the top level of threat being reserved for a full-blown crisis.

Here is an example using a straightforward numbering system:

TIER ONE/CRISIS

A significant threat, high profile with wide visibility and is already causing harm (or is highly likely to do so in the near term) to the company's reputation or business and the impact could become even more severe.

TIER TWO

Escalating issue, growing threat to become a visible crisis or have an impact on the company's brand or business operations. This might mean that there is media coverage and/or social media visibility or the issue has become known to customers and/or business partners. However, there is still the possibility that the situation can be resolved without significant damage to business or reputation.

TIER THREE

Emergent issue with potential significance to become a larger threat – but there is no immediate threat, little or no mainstream media coverage, conversation on social media or customer and/or regulatory impact.

Once you have identified these threat levels, the plan is built on this platform, with the specific content addressing a handful of key questions:

- Who takes lead responsibility for each level of threat (geography, function, corporate communications, crisis team, senior executives etc.).
- What is the system for reporting the initial incident to Corporate Communications (or whichever function is ultimately responsible for crisis management)?
- What are the initial response steps to be taken at each level of threat?
- What is the escalation procedure at each level when the situation and the threat begin to get more serious and the response must be elevated to the next level?

STEP THREE:
Tools to Support Decision-Making

To guide the decision-making in responding to an issue or a crisis—and to answer those key questions we identified in the previous section which govern the appropriate escalation of, the threat—the crisis plan should include easy-to-use guidelines, checklists and protocols that the crisis team can quickly and easily apply in the moment of crisis.

Here are examples of the kind of tools you might want to include in your plan:

INCIDENT REPORT FORM

Easy-to-use form for the person or team who first recognises the threat and must alert Corporate Communications and Legal immediately.

The Incident Report Form should collect such information as the name and contact details of the person reporting the incident, as many details of the incident as can be confirmed and the initial assessment of the seriousness of the threat.

THREAT ASSESSMENT CHECKLIST

These are questions that help the team assess at which level this threat should be treated and therefore the appropriate level of the response.

Questions would include: What happened? What is the scale of the threat? What has been the response so far? What is the potential damage to the company's reputation or business?

ESCALATION CHECKLIST

These are questions to assess whether the threat level is rising and therefore the situation should be escalated to a higher threat level with a heightened response and more expert resources.

Questions should be designed to gather more information about the level of risk and worst case scenarios in areas such as people safety, legal & regulatory, property, brand and data/IT.

MAPPING STAKEHOLDER COMMUNICATIONS

This tool identifies the most important internal (employees, investors, etc.) and external stakeholders (customers, partners, suppliers, regulators etc.) and ensure that they are being addressed in the communications and crisis response.

SPOKESPERSON GUIDELINES

It is a difficult task facing the media when your organization is facing a serious crisis. This checklist should address the best practices for delivering a message via media which may be hostile.

CONFIDENTIALITY GUIDELINES

Inevitably, if your organization is facing a full-blown crisis, highly confidential information will be handled by the crisis team as it prepares a response and builds a communications plan.

INTERNAL COMMUNICATION GUIDELINES

The employee audience is often one of the most important in a crisis and, handled correctly, can decide whether your employees remain loyal and have trust in the organization post-crisis.

STEP FOUR:
Specific Scenario-based Plans

The core crisis response protocols identified in Step Two, supported in their implementation by the Crisis Tools listed in Step Three, describe the general operating principles for the organization's issues and crisis response, no matter what the specific threat.

To extend the scope of the plan and make it actionable for the team when it is facing the highest priority situations identified in the Risk Assessment, the next task is to build plans against specific threat scenarios.

These specific scenario plans identify the sub-issues and appropriate responses at the three levels of seriousness, with particular attention and detail given to the highest level of risk, the full blown crisis.

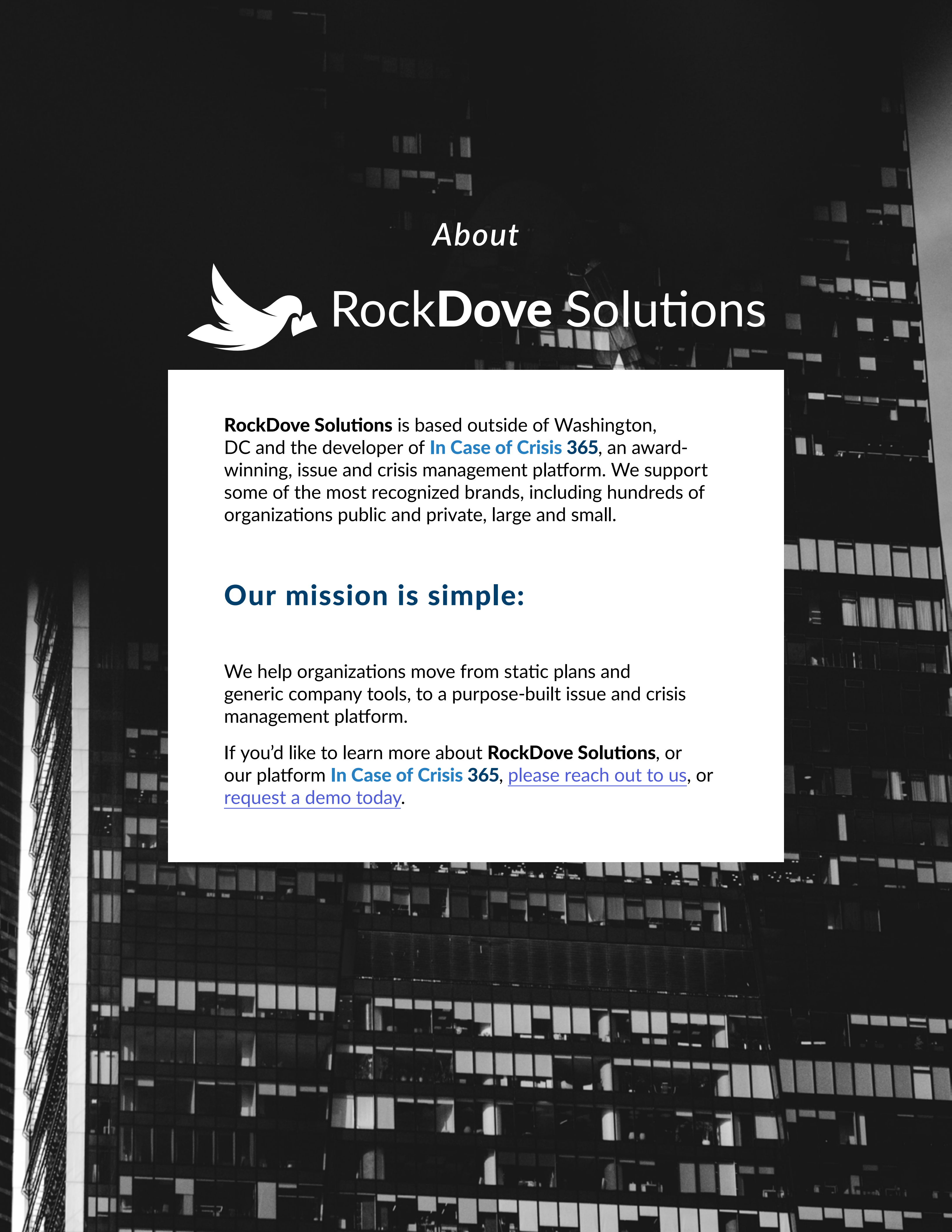
While every organization is different and the list of scenarios worthy of specific plans will vary according to the outcome of the Risk Assessment, on page 10 you'll find many of the common scenarios included in issue and crisis plans.

Ten Common Threat Scenarios

1. **Cyber-security:** threats to disrupt, hijack or illicitly gain access to all or any part of an IT network
2. **Data Leaks:** Often treated separately from Cyber-security and deals with the risks of having valuable data stolen or lost and the resultant risks to customers, trade partners, employees and the organization itself.
3. **Natural Disaster/Extreme Weather:** This scenario takes on extra importance depending on which areas of the country your headquarters, operations, or where key parts of your supply chain are based. Specific risks include hurricanes, flooding, tornadoes and wildfires.
4. **Product failures:** This covers both tangible products and service failures. The scenario begins at a level which involves a small number of customer complaints and rises all the way to a high-profile product recall.
5. **Workplace Violence/Terrorist Threats:** Sadly, these scenarios have become more common in recent years. A great deal of the work involves preparing and training employees ahead of any threat.
6. **Civil Unrest:** Another threat which has become more common in recent years and involves preparing for when your location is in lockdown and access to the company premises may involve exposing employees and visitors to potential violence.
7. **Pandemic:** The arrival of COVID-19 in March 2020 demonstrated how little prepared most organizations were for the threat of an infectious disease of that potency and scale. Pandemic will be a staple scenario in most plans for years to come.
8. **Corporate Malfeasance:** For those times when the threat comes from within the organization, with leaders, collectively or individually, doing bad things such as fraud, theft or mistreating people.
9. **Workplace Culture/Discrimination:** There has never been a greater focus and examination of workplace culture and behavior, notably policies and the management of discrimination and harassment based on race, gender, sexual orientation and age.
10. **Politics, Society & Culture:** The demands of consumers and marketing best practices puts organizations in a position where many want, or are forced, to take a position on the big issues of the day. Which means that there will be many people on the other side of the issue and with access to social media to share their viewpoint.

POSTSCRIPT: Testing and Training

Once you have the plan written, legally approved and published on the most effective platform for your organization, the next step is to test the plan and train the team.



About

RockDove Solutions

RockDove Solutions is based outside of Washington, DC and the developer of **In Case of Crisis 365**, an award-winning, issue and crisis management platform. We support some of the most recognized brands, including hundreds of organizations public and private, large and small.

Our mission is simple:

We help organizations move from static plans and generic company tools, to a purpose-built issue and crisis management platform.

If you'd like to learn more about **RockDove Solutions**, or our platform **In Case of Crisis 365**, please reach out to us, or request a demo today.