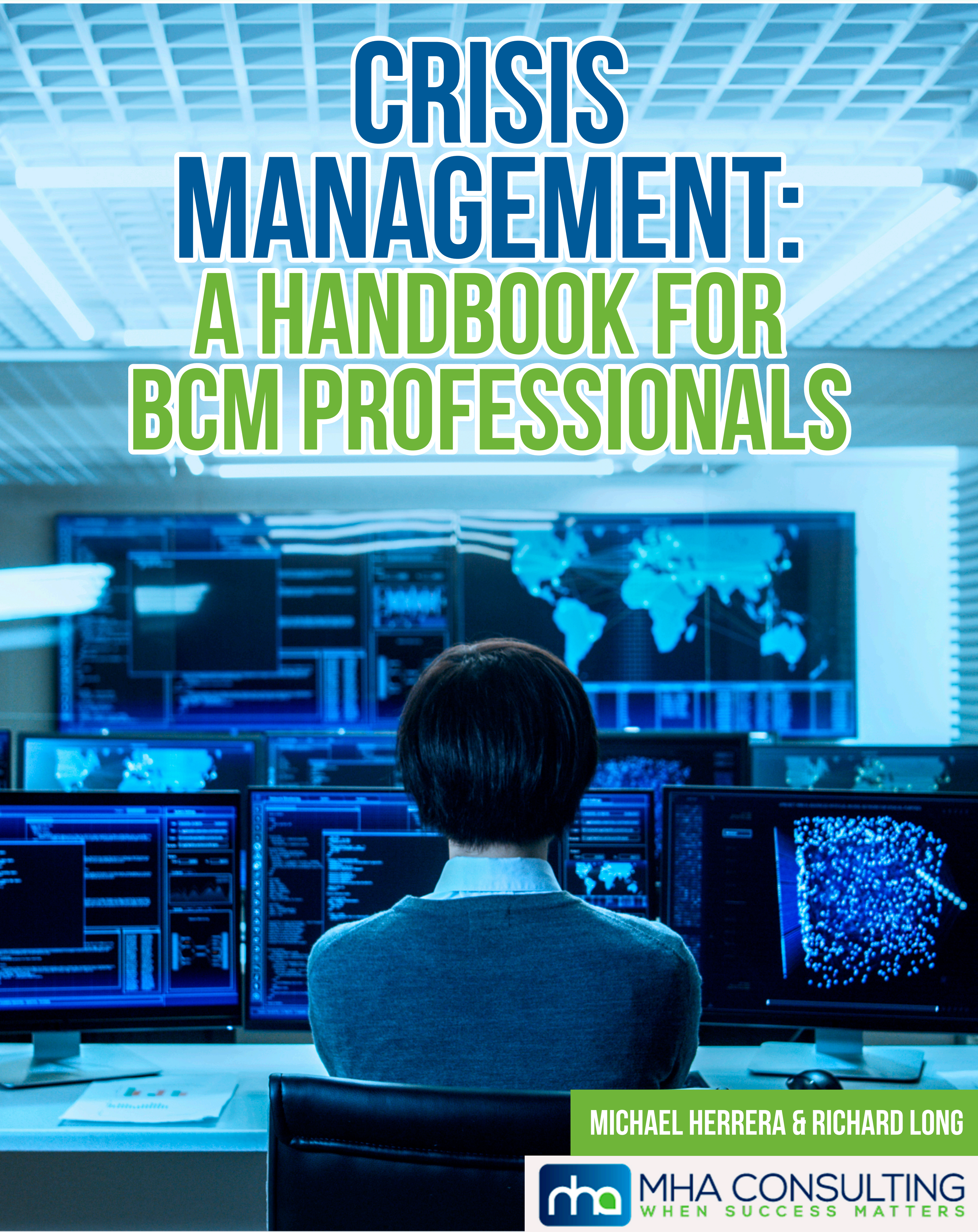
CRISIS MANAGEMENT: A HANDBOOK FOR BCM PROFESSIONALS



MICHAEL HERRERA & RICHARD LONG

MHA CONSULTING
WHEN SUCCESS MATTERS

Table of Contents

INTRODUCTION **3**
Most Organizations Are Not Prepared 3
Taking the First Step 3
Overview of this Handbook 3
Who You Are 4
Who We Are 4
Our Consulting Services 5

CHAPTER 1: CRISIS MANAGEMENT IN UNSTABLE TIMES **6**
The Trend of Rising Volatility 6
Three Contemporary Threats 6
Defining the Threat 7
Crisis Management Can Help 7
The Price of Neglect 9
Setting Up a Crisis Management Program 9
Takeaways 10

CHAPTER 2: STRUCTURING THE CRISIS MANAGEMENT TEAM **11**
The Roles of the CM Team 11
Consequences of Having the Wrong Team Structure 11
How to Structure the Crisis Management Team 11
The Incident Command System 12
Crisis Management Team Roles 13
Takeaways 15

CHAPTER 3: STAFFING THE CRISIS MANAGEMENT TEAM **16**
A Uniquely Stressful Activity 16
People Who Are Good in a Crisis 16
Choosing a Crisis Management Team Leader 17
The Politics of Staffing a Crisis Management Team 18
Takeaways 19

CHAPTER 4: DEVELOPING THE CRISIS MANAGEMENT PLAN **20**
Make Your Plan Simple and Robust 20
Key Considerations in Creating the Crisis Management Plan 20
Identifying Critical Facilities 21
Setting Up a Command Center 21
Accessing Critical Recovery Information in Crisis 22
Takeaways 24

CHAPTER 5: WRITING THE CRISIS MANAGEMENT PLAN DOCUMENT **25**
The Role of the Crisis Management Plan Document 25
Crisis Management Plan Writing Tips 25
What Does Not Belong in the Crisis Management Plan Document 25
What Belongs in the Crisis Management Plan Document? 26
Crisis Management Team Roles and Responsibilities Checklists 28
Document Logistics 30
The Crisis Management Plan Document Is the Linchpin 30
Takeaways 30

CHAPTER 6: CRISIS COMMUNICATIONS: SHARING INFORMATION, PROTECTING YOUR BRAND....... 31
Success Is Won in Advance....31
How to Communicate in a Crisis....31
The Social Media Challenge....32
How to Protect Your Brand....32
Takeaways....34

CHAPTER 7: THE ALARM SOUNDS: MANAGING A CRISIS EVENT.... 35
Chaos vs. Organized Chaos....35
Crisis Management Priorities....36
Execute Your Playbook....36
Lifecycle of a Crisis....36
Documenting the Crisis....40
Crisis Management and Crisis Leadership....41
The Crisis Ends....43
Takeaways....43

CHAPTER 8: ONCE THE SMOKE CLEARS: MANAGING THE AFTERMATH.... 44
Is It Really Over?....44
Resuming Normal Operations....44
Coming to Grips with Your Losses....45
Learning from the Experience....46
Takeaways....47

CHAPTER 9: CRISIS MANAGEMENT TRAINING AND EXERCISES: PREPARING YOUR TEAM.... 48
The Secret to Doing Well....48
The Importance of Training....48
How to Mismanage a Crisis....48
The Solution Is Training....49
Mock Disaster Exercises....49
Facilitating a Mock Disaster Exercise....51
The World of Micro Mock Disaster Exercises....53
Takeaways....55

CHAPTER 10: CRISIS MANAGEMENT METRICS: A TOOL FOR IMPROVEMENT.... 56
Metrics in Crisis Management....56
Key Crisis Management Metrics....56
Using Metrics to Improve Your Program....58
Takeaways....59

CHAPTER 11: INTERVIEW WITH A CRISIS MANAGER.... 60
Introducing Rich Robinson.... 60
Most Organizations Prefer Wishful Thinking.... 60
Few Teams are Ready for the Second Phase.... 60
Have a Single Spokesperson and Pre-written Scripts.... 61
Keep the Command Center from Becoming a Mob Scene.... 61
The CEO is Probably Not the Right Crisis Leader....62
Many Crisis Management Teams Are Confident Because They Are Uninformed....62
Takeaways....63

CONCLUSION.... 64

Crisis Management: A Handbook for BCM Professionals

INTRODUCTION

In today's turbulent world, having a strong crisis management program is vital for any organization that wants to be sure of having a flourishing tomorrow.

Trouble can strike any company, nonprofit organization, or municipality or government agency at any time.

The best way of ensuring your organization can manage an incident and come out in a viable condition is to develop a strong crisis management (CM) program. This means putting together and implementing a team, plan, and training routine to help you prepare for, navigate, and recover from an emergency.

Most Organizations Are Not Prepared

Regrettably, most organizations are not as prepared as they should be to face a crisis situation.

The reason is not because the people in charge aren't aware of the risks or don't care about their organizations. It's because they have no idea how to get across what seems to them an unbridgeable gulf between their current unprepared state and the promised land of having a strong crisis management program.

Our message in this ebook—a message drawing on our combined 60 years of experience in the fields of crisis management, business continuity, and IT/disaster recovery—is that the gap that currently exists between where you are in terms of your crisis management program and where you should be is not unbridgeable.

The gap *is* bridgeable, and in this ebook we are going to set down the steps your organization would need to take to bridge it.

Taking the First Step

A journey of a thousand miles starts with a single step. By reading this ebook, you are taking that first, single step to begin your journey of improving your organization's crisis management readiness and better protecting its future.

Overview of this Handbook

In the following pages, we are going to explain the elements that make up a good crisis management program and tell you how you can go about implementing such a program at your organization.

More than that, we are going to tell a story—a story about how a realization of the need for a good CM program can lead an organization to form a crisis management team (CMT), develop a crisis management plan, write a crisis management playbook, and ultimately to its successfully managing an event.

After that we'll talk about the issues organizations face in handling the aftermath of a crisis, the all-important role of training, and how metrics can help an organization improve its crisis response.

We will lead you to an understanding of the following specific topics:

- What crisis management is and why it is more important than ever in our age of climate change, cyberattacks, and social media mobs (Chapter 1: "Crisis Management in Unstable Times")
- The consequences of structuring your CMT the wrong way and how to do it right (Chapter 2: "Structuring the Crisis Management Team")
- How to find the right people for the CMT and what to look for in a team leader (Chapter 3: "Staffing the Crisis Management Team")
- How to develop a crisis management plan, identify your critical facilities, and set up a command center (Chapter 4: "Developing the Crisis Management Plan")
- How to get your plan down in writing and the importance of creating checklists for the various team roles (Chapter 5: "Writing the Crisis Management Plan Document")
- How to share information about the crisis with stakeholders and the media while also safeguarding your organization's brand (Chapter 6: "Crisis Communications: Sharing Information, Protecting Your Brand")
- How the CMT should go about managing an incident once trouble starts (Chapter 7: "The Alarm Sounds: Managing a Crisis Event")
- The problems that come up after an emergency and how to handle them (Chapter 8: "Once the Smoke Clears: Managing the Aftermath")
- The secret to helping your organization's CM team develop skill and confidence in managing emergencies (Chapter 9: "Crisis Management Training and Exercises: Preparing Your Team")
- How employing a few simple metrics can help your organization get better at crisis management (Chapter 10: "Crisis Management Metrics: A Tool for Improvement")
- What the big issues in crisis management look like from the point of view of someone who's spent decades as a CM practitioner, namely MHA's own Rich Robinson, who has 30 years' experience in law enforcement and was one of the first responders to arrive after the Sandy Hook school shooting (Chapter 11: "Interview with a Crisis Manager")

Each chapter concludes with a list of takeaways summing up the points you really need to know.

Who You Are

This book is intended for anyone at a private company, nonprofit organization, or in the public sector, whether their industry is heavily or lightly regulated, in manufacturing or services, who has some responsibility for their organization's crisis management program, or who has an interest in evaluating or strengthening that program.

We think you will find what we have to say valuable whether your perch on the org chart is as a senior executive, business continuity professional, or something else.

From time to time in the ebook, we use phrases such as "your team," "your plan," and "your command center." What we mean by that is *your organization's* team, plan, and command center.

Who We Are

We are the CEO and founder of MHA Consulting (Michael Herrera) and a senior advisory consultant at MHA (Richard Long). We previously coauthored the ebook *Your BIA Action Guide: A Handbook for BIA Professionals*, and Michael is the author of the ebook *10 Keys to a Peak-Performing BCM Program*.

As CEO of MHA, Michael has led MHA to becoming a leading provider of Business Continuity and Disaster Recovery services to industry-leading organizations on a global level. He is also the founder of BCMMETRICS, a cloud-based suite of continuity tools designed to help BCM professionals build comprehensive programs. Prior to founding MHA, he was a regional VP for Bank of America, where he was responsible for business continuity across the southwest region.

Richard is one of MHA's practice team leaders for technology and disaster recovery related engagements. He has been responsible for the successful execution of MHA business continuity and disaster recovery engagements in industries such as energy and utilities, government services, healthcare, insurance, risk management, travel and entertainment, consumer products, and education. Prior to joining MHA, Richard held senior IT director positions at PetSmart (NASDAQ: PETM) and Avnet, Inc. (NYSE: AVT).

Our Consulting Services

For those interested in learning more about MHA Consulting's services or the business continuity software products produced by BCMMETRICS, our contact information is below. We're always glad to discuss how our services and products can help organizations of all kinds become better at crisis management and more resilient overall.

Michael Herrera, CEO (herrera@mha-it.com) and
Richard Long, Senior Advisory Consultant (long@mha-it.com)
MHA Consulting

CHAPTER 1: CRISIS MANAGEMENT IN UNSTABLE TIMES

As everyone who has ever stubbed their toe knows, the world can be a dangerous place.

Business is not immune to this reality. In fact, sometimes it seems to have a big target painted on its back.

Crises and emergencies happen all the time in the world of business and organizations. Equipment catches fire, chemicals leak, roofs collapse. Storms hit, sinkholes open, and people on company premises trip and are injured or become ill. Sometimes people representing the organization act inappropriately or unlawfully, bringing bad publicity and the attention of law enforcement. Sometimes disturbed people perpetrate acts of violence, turning offices, factories, and warehouses into crime scenes and places of tragedy.

The Trend of Rising Volatility

As if the standard shocks of life weren't enough, in many respects the world today is growing more unstable. Numerous trends are raising the frequency and consequences of emergencies.

These trends are not limited to the United States. Many experts believe the entire world is entering a period of increased volatility.

To compound the problem, these days our global dependencies make us susceptible to upheavals a world away.

Three Contemporary Threats

Three threats loom largest in terms of the trends elevating the risk level for business. They are: climate change, the proliferation of cyberattacks on company computer networks, and the rise of social media.

Climate Change

The reality of climate change is something no prudent leader can ignore. This reality is illustrated by the stories of extreme weather events that have come to dominate the news in recent years. This includes the fires that have affected large areas of California, the hurricanes in Puerto Rico, Florida, and the Bahamas, and record-setting flooding in places as far apart as Houston, Texas, and Venice, Italy.

This anecdotal evidence is borne out by studies and data. This type of weather has brought serious emergencies to many organizations. It brings a realistic possibility of them to many more.

Cyberattacks

Another trend that is creating new danger for business is the increase in cyberattacks. Over the past generation, we have become dependent on computer networks for doing business and running our organizations, but those networks are increasingly vulnerable to attack.

Every week brings a new story in the news about a municipality wrestling with whether to pay a ransom to hackers who encrypted their data or a corporation that has suffered a data breach and the exposure of their customers' private information.

The cost of such problems can be enormous, including the inability to provide services, loss of consumer confidence, reputational damage, legal liability, and penalties from regulatory authorities.

Social Media

The third trend raising the risks faced by business is the rise of social media.

Traditionally, we think of an emergency as a situation where first responders come to our facility with their lights flashing. Social media crises are not accompanied by the sound of sirens, but they have just as much potential to harm your organization as any flood or fire. On Twitter and other platforms, complaints against your organization can spread like wildfire, no matter what their proportion of fact to fiction.

A social media mob can damage a company like nothing you've ever seen. It can drive media coverage, boycotts, and similar events that can cause lasting damage. Thanks to Twitter and Facebook, a seemingly minor problem can become an existential crisis in the blink of an eye. Problems that in the past might only have been known to a small number or people can go viral within a few hours.

Today any discussion of crisis management for business must address the issue of a social media driven reputational crisis.

Defining the Threat

Throughout this book, we'll talk in general terms about crises and emergencies that might strike your company. Before we get too far, it might be helpful to define the threat by listing of some of the actual, specific emergencies your company might face.

Here are some of the crises that will almost certainly strike one or more organizations somewhere in the country within a short time of your reading these words (some will be more relevant to your organization than others):

- Cyberattack
- Reputational damage
- Flood
- Hurricane
- Tornado
- Structure fire
- Wildfire
- Earthquake
- Toxic gas release
- Chemical spill
- Explosion
- Civil disturbance
- Workplace violence resulting in bodily harm and trauma
- Loss of Utilities (Power, Water, etc.)
- Ransomware attack
- Leak of embarrassing internal communications
- Liability for customer injury or death
- Loss of data center
- Loss of key people
- Company leader charged with wrongdoing
- Bomb threat
- Accident involving motor vehicles
- Pandemic
- Terrorist attack

We give this list not to keep you up at night, but to help you think about your organization's readiness and to motivate you to get prepared.

Crisis Management Can Help

The high and growing level of the threats business is facing is a reality. But here's another reality, and it isn't nearly as grim.

Organizations do not have to sit around twiddling their thumbs waiting to get damaged by the next crisis that comes along. They can do something about it.

They can't prevent every crisis, but they can ensure they are well-trained and prepared to respond when they come, thus reducing the damage they will experience. In short, they can design and implement a good crisis management program.

What Is a Crisis Management Program?

A crisis management program is a collection of organizational arrangements, plans, and training exercises that are established in advance to help a company respond effectively to emergencies.

Crisis management (CM) provides the strategic framework to centrally coordinate and direct the organization in the event of an unplanned disruption. It develops a comprehensive process that incorporates the company's internal and external resources to respond to a disruption.

A CM program sets up a team to manage crises and a plan for responding to them.

The plan addresses the whole range of crises that might impact the company, whether the causes are natural, technological, or human.

Crisis Management Priorities and Training

During an emergency, a crisis management program has four critical priorities. These are, in order of importance:

- Protecting life safety
- Stabilizing the incident
- Protecting and preserving property
- Recovering the business

A CM program includes training and exercises for the employees so everyone knows their role and is capable of carrying it out.

The Elements of a Crisis Management Program

A good crisis management program incorporates the following elements:

- **Crisis management team.** Includes a leader, primary members, and alternate members. Members should be drawn from a variety of key departments that cross-functionally represent the company.
- **Crisis management plan.** A comprehensive plan to direct the team and its response.
- **Crisis management plan document.** The written document setting forth the CM plan. Includes checklists to guide team members in responding to the crisis.
- **Crisis communications plan.** An important subpart of the CM plan. Outlines the steps that will be taken to convey the appropriate information internally and externally.
- **Command centers.** Includes physical and virtual command centers where the team can assemble during a declared event.
- **Training and exercises.** Instruction and mock-disaster exercises to improve the staff's ability to implement the CM plan and respond to emergencies.
- **Maintenance.** The CM process and documents should be regularly reviewed and maintained.

Achieving "Organized Chaos"

One thing a CM program cannot do is eliminate the stress and confusion that occurs when there is a crisis. However, a CM program can turn the scene from chaos into "organized chaos."

In organized chaos, things appear confusing and there might be a fair amount of stress, but there is also a tested, familiar, underlying structure in place to guide the company and team's response.

Experience shows this is what makes the difference between companies that get knocked flat on their back by crisis and those that respond effectively, limiting the damage and quickly getting back to work.

The Price of Neglect

Unfortunately, many organizations do not take advantage of the tools crisis management provides to help in managing emergencies.

They prefer living with their heads in the sand.

Here are some examples of the kind of neglect we often see while working as crisis management and business continuity consultants:

- Perhaps 75 percent of companies are unprepared.
- Many people in positions of responsibility take a casual attitude toward crisis readiness.
- Too often, what drives the approach to CM is the shortness of people's attention spans, not the importance of the issue.
- Many leaders assume their staff will do fine operating by the seat of their pants if and when crisis strikes.
- Even many companies that have CM teams don't conduct the necessary training, exercises, and maintenance. These companies have CM programs in name only.
- At a large number of companies, many people have no idea where they should go if an emergency forced them to evacuate or relocate.

This kind of neglect comes with a price.

When emergencies occur, companies that aren't prepared tend to learn the hard way that lack of readiness:

- Leads to greater impacts on people's lives and safety.
- Leads to greater damage to property.
- Increases the amount of time needed for normal operations to resume.
- Increases the chances the company will never recover.

Staff who are winging it in situations of high confusion and great pressure have a high tendency to take steps that make the situation worse and to miss steps that could make it better.

Setting Up a Crisis Management Program

Organizations of all types and sizes should make adequate preparations for managing crises.

Not only that, but they can do it. It's not hard or expensive.

Dealing with a crisis might be a high-stakes, high-tension affair but setting up a crisis management program is relatively easy and stress-free. It doesn't require that anyone be an action hero. It only requires that the people in charge be patient, diligent, and follow through.

If you start now and work on it bit by bit over time, eventually you'll get to where you need to be.

Spending on crisis management is money well-spent. Being prepared minimizes the impact of the event and heightens the potential for you to respond and recover the business sooner, with fewer impacts to your stakeholders.

A Responsible Approach to Crisis Management

Your goals as a company that takes a responsible approach to crisis management should be:

- To have a well-trained, cross-functional crisis management team.
- To have a defined CM process, methodology, and plan.
- To conduct regular CM training for staff and raise awareness of the CM plan and program.
- To hold regular mock disaster exercises to stress-test the program and challenge team members.
- To keep the CM plans and documentation up to date.

Sooner or later, every company is hit by crisis. It's a matter of when, not if. Your company will be impacted by an unplanned disruption at some point. You can choose to be prepared or not.

You need to get your CM planning started today, not tomorrow. It is better to implement 75 percent of a plan and strategy right away than to wait with the goal of implementing 100 percent at a later date.

Organized chaos is much better than chaos.

These days it's more important than ever that your organization be ready for trouble before it strikes.

By following the steps set forth in this ebook, you can ensure that your organization will respond swiftly and effectively the next time trouble comes to call.

Takeaways

- Organizations today face many threats, including from the new trends of climate change, social media, and the rising rate of cyberattacks.
- A sound crisis management program can help an organization take control of its fate and turn chaos into organized chaos, if and when it is faced with an event.
- Most companies are unprepared, but the responsible thing to do is to begin setting up a good crisis management program.

CHAPTER 2: STRUCTURING THE CRISIS MANAGEMENT TEAM

The way you structure and staff your crisis management team (CMT) is the make-or-break factor in terms of how well your organization does at setting up a CM program and steering the organization through an emergency.

In this chapter we'll look at the best way to structure the CMT. The topics of how to choose the right people to lead and staff the team will be covered in the next chapter.

The Roles of the CM Team

The crisis management team has two roles. It helps the organization develop the crisis management plan and it navigates the organization through emergencies.

In responding to a crisis, the team collects and swiftly analyzes information then makes decisions, takes actions, and coordinates the responses of various departments throughout the company.

The team tries to ensure that the right people take the right actions at the right time, based on the impacts the event is currently having and on potential future impacts.

Team Commitment

The CMT should be committed in the highest degree to achieving the goals of the crisis management plan, such as protecting life safety, containing the event, protecting property, and expeditiously resuming normal business operations.

Consequences of Having the Wrong Team Structure

It's hard to overstate the problems that can arise from having a poorly structured CMT.

A poorly structured team is one whose membership is not drawn from the correct departments and that lacks a sufficient number of primary and alternate members.

A poorly structured team will lack access to needed expertise at the right time, whether it's in developing the crisis management plan or executing it during an emergency.

A poorly structured team might have many people whose skill and knowledge sets are redundant or unnecessary, creating confusion and increasing friction.

Having a poorly structured CMT can result in poor decision-making and delayed or paralyzed decision-making, with all the consequent impacts to the organization's safety, property, recovery, and reputation.

How to Structure the Crisis Management Team

Structuring a crisis management team is very straightforward. Every team should have the following levels of personnel:

- **Leader.** Manages the team, has final decision-making authority, provides for the safety and well-being of the employees.
- **Core team members.** People that are involved in responding to every crisis. Representatives of key departments.
- **Extended team members.** People whose participation depends on the size and nature of the emergency. Representatives of peripheral departments.

In addition, alternates should be designated for every role: leader, core members, and extended members. Large organizations should consider having multiple alternates, especially for the most critical roles, such as CMT leader.

Having alternates ensures there is always a qualified person available to assume the role. In the case of prolonged crises, it allows staff time to rest and recuperate between shifts. People can work only so many hours in a day and all of us reach a point where our ability to make good decisions declines.

Core Team vs. Extended Team

The CMT should include a core group that is notified for every emergency and others who are brought in as circumstances require. The core group typically includes the leader and the people responsible for facilities, security, human resources, communication, and legal affairs. These individuals make an initial assessment then scale the team up as necessary. Members of the extended team are brought in when the scale and nature of the emergency affects their area of expertise and a larger response is warranted.

Multiple Crisis Management Teams

An organization might have multiple CM teams, for example a general, enterprise-wide crisis management team, an IT-only team, an operations-only team, a supply chain team, and so on. The specialized teams report up to the enterprise-wide team.

Trained in Advance

There should not be anything ad hoc about the CM team. The structure and membership should be determined ahead of time. The members should know their roles and be trained in them before being called on to perform in an emergency.

The Focus of Each Member

Each person acts as an advocate for his or her role. They gather information on that area and make sure the impacts to that area are understood and given due priority. Each member leads or directs the recovery or actions for their area and documents what is going on there. Members should also understand that sometimes other areas will be given priority.

Small Companies vs. Large Companies

The basics of structuring a CMT are the same at small and large companies. The biggest difference is, at smaller companies one person might perform multiple roles. The important thing is making sure that each area has someone assigned to look after it.

A Common Mistake

A common mistake we see is that organizations bring in too many people too soon. The result is the command center fills up with people who have nothing to do. The smart approach is to bring in the core team first and scale up as events require.

The Incident Command System

Most organizations leverage the Incident Command System (ICS) in organizing their crisis team and program. (Others prefer to stick with their traditional corporate hierarchy.)

ICS is a well-known system for managing incidents that has been adopted and recommended by many government agencies including the Federal Emergency Management Agency and the Department of Homeland Security.

ICS consists of a standard management hierarchy and procedures for managing temporary incidents of any size, scope, or complexity. (There's a version called the Hospital Incident Command System, or HICS, which is especially for healthcare organizations.)

ICS provides an organizational structure for incident management and a guide for planning, building, and adapting that structure. It is very flexible. An organization can use as much or little of the ICS structure as is compatible with its size and mission.

The ICS structure is built around five major management activities or functional areas:

- **Command.** Includes Incident Commander, Safety, Liaison, and Communication. Sets priorities and objectives and is responsible for overall control of the incident.
- **Operations.** Accountable for all tactical operations necessary to carry out the plan.
- **Planning.** Responsible for the collection, evaluation, and distribution of information regarding incident development and the availability of resources.
- **Logistics.** Responsible for providing the necessary facilities, services, and materials to meet incident needs.
- **Finance/Administration.** Responsible for monitoring and documenting all costs while providing the necessary financial support related to the incident.

For more on the Incident Command System, see "Command Performance: Using the Incident Command System (ICS)," by Richard Long, on the MHA Consulting web site (https://www.mha-it.com/2018/02/21/ics/).

You can also search Incident Command System on the internet to learn more about this proven method of organizing for crisis response.

Crisis Management Team Roles

The CMT is divided into a core team and an extended team. The makeup of the core team will vary from organization to organization. One of the key factors in determining who should be on the core team at a given company is the industry it is in.

Core Team

The following are roles that are commonly included on the core crisis management team:

- **Team Leader.** Manages the team and provides for the safety and well-being of the employees. Is the team facilitator, not its dictator. Encourages discussion and debate to ensure that important matters receive due consideration. Keeps the group moving forward and guides the members toward decisions which have broad support. Has the final authority and may be required to make a decision quickly and with limited information. Facilitates the timely resumption of business operations to minimize the impact of the emergency on customers and shareholders.
- **Administrative Support.** Supports the team leader and members. Knows where everything is and how to get things done. Takes notes and keeps track of action items and open issues. Knows how to obtain food and transportation, line up hotel rooms, and keep everything moving. The importance of this role should not be underestimated.
- **Finance and Administration.** Manages the organization's financial stability during an event. Understands the impact of the crisis on finance and accounting matters, including business process issues and regulatory compliance and reporting. To help the organization get through the crisis, the person in this role might seek raises in credit limits or delay some types of reporting.

- **Human Resources.** Responsible for developing and implementing services that support affected employees during the event. Responsible for temporary staffing, benefits issues, and bringing in grief counselors, if necessary. In coordination with other departments such as Communications, helps in keeping employees informed about the crisis (for example, by notifying employees that all overtime requests are approved for the next two weeks).
- **Information Technology.** Tracks and manages how the event impacts the company's IT functions. Directs the IT team as it works to restore affected computer systems and networks. Informs the crisis management team of the event's impacts on IT as well as the likely impact of any actions that might be taken to deal with the crisis. For example, if the CMT was considering shutting down a building as a result of a fire, the IT person could advise the team as to what the impact would be on the organization's computer systems and processes.
- **Legal.** Provides advice and legal support to all CMT members with regard to liability, communications, lawfulness, prudence, and the legal ramifications of actions that might be taken. Can advise on whether certain strategies under consideration are permissible. Might advise the team about such legal matters as the need to protect evidence.
- **Operations and Business Recovery.** Serves as liaison between the CMT and the business recovery teams. Likely to have a lot of input in the actions of the team overall. Can provide the team with information on how the crisis is impacting the organization at retail stores, distribution centers, or manufacturing facilities. Can help the team evaluate proposed courses of action from the operations point of view. For example, if it is thought necessary to change the schedule of the distribution center, the ops person can address the downstream impacts of the change.
- **Project Management Office.** Supports the CMT through understanding the impact of the crisis (and any steps taken to deal with it) on the various projects the organization has underway. Can advise the team on which projects can be stopped or delayed with minimal impacts and which would bring higher impacts.
- **Risk, Security, and Compliance.** Advocates for the teams dealing with risk, compliance, and security at the organization (including physical security and data security). Works closely with local, county, state, and federal law enforcement and investigative agencies. Advises the team on whether any contemplated action might put the organization out of compliance with regulations from OSHA or other agencies. Makes sure the team attends to the security impacts of proposed actions. For example, if someone wanted to leave the exterior doors in a facility open for some reason, they would point out the need to station people there to protect those entrances.
- **Facility Support.** Responsible for conducting an assessment of the damage to facilities caused by the event. Makes sure issues related to the organization's buildings are given proper consideration. Attends to such issues as whether the buildings are safe and accessible and whether it's necessary to move employees to other facilities.
- **Corporate Communications.** Considers the impact of the crisis and any proposed responses on the communications functions. Works with other departments such as Legal, Operations, and Human Resources to ensure consistency in communications throughout an event. This includes communications to staff, shareholders, the media, and Wall Street. Tackles such issues as what to communicate and to whom if the crisis causes loss of life.

Extended Team

Extended team members are those from more peripheral departments. They are brought in as needed depending on the scale and details of the emergency.

At some organizations, some of the roles listed above as core might be considered part of the extended team.

By the same token, some roles that are grouped with the extended team at some companies might be on the core team at others.

Roles commonly seen on companies' extended CM teams include Operations, Manufacturing, Customer Service, R&D, Marketing, Sales, Logistics, Retail, Vendor Management, and people representing remote locations.

Takeaways

- A crisis team should consist of a leader, a core team made up of representatives of the most central departments (such as HR, Operations, Finance, IT, and Legal), and an extended team of members of more peripheral departments who are brought in as necessary.
- Expand the team as the crisis grows and contract the team as it subsides.
- The Incident Command System (ICS) is an excellent way to organize your team and program.

CHAPTER 3: STAFFING THE CRISIS MANAGEMENT TEAM

No factor is more important in determining the success or failure of a crisis management program than the people chosen to implement it.

The consequences of having a poorly staffed and led CM team in charge during a crisis can be severe. They include sluggish, paralyzed, and poor decision-making and the resulting negative effects on the organization's safety, property, recovery, and reputation.

In this chapter, we'll look at the following aspects of putting together a crisis management team:

- The uniquely stressful environment of working on a crisis team
- The characteristics that make people good in a crisis and how to find individuals who have them
- What to look for in choosing a crisis team leader
- The politics of staffing a crisis management team
- How to manage a crisis team

A Uniquely Stressful Activity

Working on a crisis team is a uniquely stressful activity. All of the ordinary pressures of organizational life are intensified owing to the time pressure, high stakes, and uncertainty.

Imagine working in a command center during a crisis. Reports of damage and casualties are flooding in. Confusion is widespread. Information from outside might be scarce or contradictory. Your colleagues on the CM team might disagree with you and each other in their assessments of what's going on or their opinions of what should be done. Some people might be emotional or short-tempered. The media is after you for information and social media is blowing up on you. You might have to make hard trade-offs about what to save and what to sacrifice. Action is imperative but you have little or no time to think.

In a crisis, high-stakes decisions must be made quickly, often in circumstances of great confusion. This is a task unlike any other role in business.

People Who Are Good in a Crisis

We all know that some people are good in a crisis and others give way to emotion or become paralyzed with fear. Most people probably fall in the middle of the range.

One of the most important things to look for in staffing your CM team is people who can keep their heads and perform effectively in situations of chaos, confusion, and loss.

One of the things to avoid is picking people who are inclined to fly off the handle or crumple under pressure.

Paradoxically, many people who excel in day-to-day business life are liabilities when the task at hand is managing a crisis. By the same token, some individuals who might go overlooked in daily work life might have just the quality of grace under pressure that is desirable in a crisis situation.

In choosing the leader and members for a crisis team, it's important that you understand what the job involves and pick people who have the skills necessary to perform it.

Characteristics Aligned with Crisis Aptitude

People who are effective in crisis situations tend to have the following characteristics:

- Can swiftly make determinations and decisions based on the information available at the time
- Are confident but not egotistical
- Have tactical knowledge
- Are good at solving problems
- Are willing to act in the absence of consensus
- Are calm, level-headed individuals who are not overly sensitive to criticism or debate
- Are collaborative. Work well with people from other departments

Emergency situations are inherently stressful and time-pressured. Performing effectively in the crisis management role calls for a unique temperament and skill set.

Finding People with the Right Characteristics

We often find that in large organizations some of the best crisis management people are the direct reports of the senior leadership team. Another good way of identifying people who are good in this role is to keep an eye out for who comes to the forefront during business continuity exercises.

Most people have a sense of who in their department is a level-headed, can-do person capable of working well with others. Ask around and identify these individuals.

Becoming a Cohesive Unit

As your team comes together, there's a lot to be said for striving for stability in its membership. With most teams, the longer they work together, the more cohesive they become. A NASA study has found that teams whose members have been together for a long time are more efficient and effective than teams whose rosters are in constant flux.

Choosing a Crisis Management Team Leader

A good CMT leader has all the qualities of an ordinary crisis management team member and more. Choosing the right person to lead your team—and strong alternates to back that person up—is one of the most significant factors affecting the success of your CM program and crisis response.

In seeking a CMT leader, you are seeking a person to entrust with the task of guiding your organization through an incident. The CMT leader should not be chosen based on seniority, job title, or any other extraneous factor. They should be selected solely on the basis of having the right skills, knowledge, and temperament for the position.

Select someone who is a good fit for the role. Note that this is very different from saying, choose the senior person on the CM team or choose the person who lobbies hardest to get the job.

Managing a department well on a day-to-day basis and being able to manage the team through a crisis are two very different tasks.

Two Approaches to Choosing a Leader

There are two common approaches to choosing a crisis team leader:

- Identifying a leader (and alternates) who will be in charge regardless of the situation. Should be a strong leader with general knowledge of all areas.

- Choosing the leader for each incident based on who has the most expertise in the affected area. For example, a Facilities person in the event of a fire and an IT person in the event of a cyberbreach.

Characteristics of a Good CMT Leader

In addition to the qualities given above for all crisis management team members, the CMT leader should be:

- **Respected.** Is well-respected within the organization and thought of as a good leader.
- **Knowledgeable.** Has a solid high-level understanding of the business, its operations, and its continuity plans.
- **Adaptable.** Can adjust to changing situations quickly and think outside the box.
- **A good facilitator.** Is able to lead the team as well as let others lead when their expertise or knowledge is more relevant.
- **A good listener.** Listens to others' input to make the best decisions. Knows when to end discussion and move on.
- **A decision maker.** Makes the tough decisions when no one else wants to then sticks with them.
- **Strategic.** Thinks on an enterprise level. Delegates tactical tasks to those below for execution.
- **Organized.** Keeps the team on track and focused on the event at hand. Allows others freedom to think but resists letting the team be diverted from the mission.
- **A risk analyzer.** Works with the team to assess the most critical risks, define a high-level action plan, delegate tactical execution, and monitor progress.
- **Committed.** Willing to be the leader. Committed to learning the CM process and mastering how to lead an organization through a crisis.

The Leader Sets the Pattern

The CMT leader's style and personality strongly influences the conduct of the team. This is another factor to keep in mind when choosing the person to head your team.

If you pick someone calm, resolute, and resourceful, those characteristics are more likely to be brought out in the team as a whole.

If you pick someone who values the contributions of others, the members are more likely to make their best effort.

If you pick someone capable of making tough choices in the absence of consensus, the team members are themselves more likely to display realism and pragmatism.

But if you make the mistake of picking as a leader someone who complains that the incident doesn't match the CM plan and throws up their hands, your team might show equal helplessness and lack of fight.

The Politics of Staffing a Crisis Management Team

Many and perhaps most crisis management teams have their fair share of politics, alliances, and rivalries among the people from senior management who typically fill the leading roles.

Serving on the CMT is commonly seen as badge of status and importance and as a result, high-ranking people often wish to serve on it, regardless of whether they possess the desired characteristics. Needless to say, unsuitable people contribute little to the team and often impair it.

A high-ranking person who lacks the requisite qualities is not a good fit for the CM team no matter how much he or she would like to be on it.

Staffing the Team by Title vs. by Capability

There are two common ways of selecting who from the various departments will represent the department on the CMT, by title and by capability. Staffing by title is when people are chosen based on their job title or seniority. Staffing by capability is when they are selected based on aptitude.

We've already discussed the uniquely stressful nature of the CM challenge and the qualities that enable certain people to perform with high competence in that situation.

We strongly believe that crisis management teams should be staffed by capability.

The stakes in crisis management are too high to choose the CM team leader and members by any criteria other than each person's being knowledgeable, collaborative, and cool under fire. If the senior person in a department has those qualities, great. If not, then someone else should represent the department on the CM team.

We recently had a client that staffed its CM team by title then experienced a crisis that exposed the team's inadequacy. Having learned its lesson, the company moved the high-ranking but unqualified people off the team and brought in lower-ranking but better suited individuals. As a result, the organization now has a highly competent team in place to deal with future emergencies.

We encourage everyone who has a role in staffing a CMT to look beyond title and bring in people who can truly do the job.

Office Politics Workarounds

There are some ways of mitigating the negative effects of political appointments on the functioning of the CM team.

One method is to bring in additional people who can do the work. If a high-ranking person must be included on the team for political reasons, consider also bringing in a lower-ranking person from the same department who has the skills and qualities needed to do the job.

Another workaround is to find the political appointee a role on the team suited to their expertise and temperament. Suppose the person wanted to be the team leader but lacked the necessary characteristics. Perhaps they would be satisfied with taking a role as an ordinary team member.

Sometimes senior management is open to persuasion when it comes to whether to staff by title or by capability. If those organizing the CMT point up the stressful aspects of the CM process, and emphasize the importance of choosing people who are cool under fire over those with the most pull, management might see the light. At any rate, it's worth a try given how important the performance of the CM team is to the fortunes of the organization.

Takeaways

- ◘ In staffing a CM team, it's important to choose people who can function well in the confusing, pressure-cooker environment of a crisis.
- ◘ The all-important role of team leader should be filled by someone who is respected, knowledgeable, flexible, and organized, as well as cool under pressure.
- ◘ Staff your team based on ability not seniority and do your best to manage the inevitable political pressures.

CHAPTER 4: DEVELOPING THE CRISIS MANAGEMENT PLAN

A crisis management program and plan are not things a company can buy off the shelf. Every organization is different in terms of its industry, facilities, and culture.

One of the first things a company must do in developing a crisis management plan is look in the mirror. The organization needs to determine what kind of team and program structure will work best for them.

Regardless of how your company decides to organize its program, one point should be top of mind: the plan you create must be easy to read, easy to use, and be executable.

In this chapter, we'll survey some important general topics in creating your CM plan, including setting up a command center, identifying critical facilities, and ensuring you can access critical information during a crisis.

We'll look at producing the written CM plan in Chapter 5, "Writing the Crisis Plan Document."

Although we treat developing and writing the plan in separate chapters, it makes sense to perform these tasks at the same time.

Make Your Plan Simple and Robust

In creating a crisis management plan, it is helpful to keep in mind that crisis situations are unique in terms of the high levels of stress and confusion that occur during them. Your plan needs to be simple and robust enough work in that type of situation.

If conducting business under ordinary circumstances is like driving a vehicle at a moderate speed on a paved four-lane highway, managing a crisis is like driving fast over rough terrain. True off-road vehicles are engineered for heightened durability. Your crisis management plan needs to be similarly engineered.

Overcoming Inertia

The team tasked with creating the crisis management plan will probably encounter a great deal of inertia in their colleagues who are not responsible for developing the plan. Those people's cooperation is needed but can be hard to obtain. It is difficult to get people to care about crisis management until they are actually in a crisis. The simpler your system and arrangements, the easier it will be to get people to learn and use them.

Key Considerations in Creating the Crisis Management Plan

Because every organization and industry is different, there is a limit to the advice that can be offered in a guide of this kind.

However, we can set forth the general problems that you will need to grapple with and develop solutions for.

The following are some of the key matters you should think about as you start creating a crisis management plan for your organization:

- In the event of a crisis, what will the procedure for notifying the CM team be?
- What will be the procedure for activating the CM plan?
- Once a crisis has been declared, how will the CMT be mobilized?

- Who will have the authority to declare a disaster and activate the recovery process?
- Where will your primary and alternate command centers be located? (See below for more information on setting up command centers.)
- What video conference line will be used to support the CMT?
- Who will the primary and backup members be for every team role?
- How will the crisis and response be documented?
- What will the roles and responsibilities look like for each team role?
- Once the crisis is over, what procedure will be followed to formally demobilize the team and resume normal business operations?
- How and when will you conduct a post incident analysis and document the "Good, the Bad and the Ugly"?

Identifying Critical Facilities

One of the most important steps in developing your plan is identifying your critical facilities. You can't protect every facility first or make every one your top priority.

Identifying which facilities are most important to the organization's well-being gives you a rational basis for favoring some facilities over others in your CM plan.

We recommend that you sort your facilities into the following three categories:

- **Critical.** Facilities whose loss or disruption would cause high negative impacts on the organization's operations, revenue, or reputation.
- **Important.** Facilities less vital than the critical ones, but whose loss or disruption would still cause meaningful impacts.
- **Other.** All facilities that aren't considered critical or important.

What should you look at in determining how to categorize each facility? Consider what the impact would be if that facility went down. How would the loss affect your employees, operations, revenue, and reputation?

By looking at each facility in these terms, you can develop a rational basis for deciding what level of protection it should receive.

Setting Up a Command Center

You will also need to establish a command center—a place where your CM team can gather to organize itself and manage the crisis. In fact, you will want to set up three command centers. They are:

- **Primary command center.** Your principal, first-choice, go-to incident command center.
- **Alternate command center.** This should be at a physical distance away from the primary center. It's a location your team can use if the primary center is impacted and which won't be impacted by the same event.
- **Virtual command center.** A preestablished meeting place on a service such as Skype or GoToMeeting. Can be used if the team cannot use or access one of the physical centers, or if the incident happens in the middle of the night.

The following are the essential features of a physical CM command center:

- It must be large enough to accommodate everyone who is expected to work there.
- It can be locked and made secure.
- It has adequate computer, network, and telecommunications technology.
- It has conference rooms around it that can be used by members of the CMT as they manage the crisis.

For more information on setting up a physical command center, see the interview with Rich Robinson in Chapter 11, "Interview with a Crisis Manager."

Accessing Critical Recovery Information in Crisis

Another key aspect of creating a CM plan is making sure the team can access critical recovery information during a crisis.

At many companies, incidents are made worse because the CMT does not have ready access to vital, up-to-date data or even know where it resides.

Missing information causes delays while the team tracks down the absent data or conducts redundant analyses to figure it out. Incorrect information can lead to wasted effort, sow confusion, and introduce errors.

Your crisis management team shouldn't have to perform a scavenger hunt to get the information it needs.

What the Crisis Management Team Needs to Know

The following is a list of the information the CMT needs in order to effectively manage an emergency:

- Information on the severity of the impact to the organization's business processes
- Information on how long the crisis is likely to last
- Facility information
- Internal contact lists
- External contact lists
- Documentation listing the members of the crisis and recovery teams and stating what their responsibilities are
- Listing of what is critical and what is not and when it needs to be restored
- Recovery plans and checklists
- Business processing criticality and requirements
- Manual processing procedures
- Information about business risks

Most likely, you have probably already documented much of the above. The important thing is to make sure the information is up-to-date and easily accessible.

Making Sure the Crisis Management Team Has the Information It Needs

Below are some tips and considerations to help you make sure your CMT will have the right information in the right place at the right time:

- ◘ Make sure your contact lists are up-to-date and accessible.
- ◘ If your CMT depends on cloud-based information, make sure your Internet access is completely redundant with no single points of failure.
- ◘ If the data is stored on Exchange or some other system, make sure there are no single points of failure for those systems. Familiarize yourself with the recovery timeframe for them. Determine whether you can you access them remotely.
- ◘ If your data is stored on paper or in soft copies on storage devices, you will need to make an effort to keep it up-to-date. Such resources are often out of date the day after they are printed or stored.
- ◘ Determine an appropriate update schedule to keep your contact lists up-to-date. Annual or bi-annual updates are not enough.
- ◘ Make sure that your contact lists identify the secondary and tertiary team members. No one works 24×7. Your secondary and tertiary team members are also critical.
- ◘ Document the chief risks to the business. This is frequently overlooked, but the crisis management team depends on this information.
- ◘ Document the business processing requirements. Identify the impacts to them as well as what processes are critical, their dependencies, and how to manually run those processes, if necessary. (Most organizations assume they can just start processing once the systems become available again. It is commonly assumed such systems are self-healing, but we have found this is usually not the case.)

Sometimes the team will have to make decisions based on incomplete information. The team will have to determine if it is reasonable to expect that the needed information can be obtained in a timely manner. If it cannot, the team must make the best decision based on the information available.

Colin Powell, one of our great American generals, has a rule of thumb called the 40-70 Rule that speaks to the problem of making tough decisions with limited information. The rule says that when you are facing a tough decision, you should wait to decide until you have at least 40 percent of the pertinent information. You should also make the decision before you have more than 70 percent of the information. If you make a decision with less than 40 percent of the information, you are shooting from the hip and will make too many mistakes. If you wait until you have more than 70 percent of the information, you are waiting too long and imposing costly delays.

Generally speaking, the more information you prepare as part of the crisis management documentation, the better the decisions that will emerge during a crisis situation.

Giving the Crisis Management Team What It Needs

Scavenger hunts can be fun, but not when you are a member of a crisis management team in need of key information to manage your organization’s response to an incident. Do your team—and your organization—a favor: make sure the team has quick, reliable access to the information they need to perform their role. When the team has such access, it can greatly limit the negative impacts of an event.

Takeaways

- Examine the list of key considerations given in the chapter to see what your crisis management plan needs to address.
- Your plan should classify your facilities into critical, important, and other so you know how much protection to give each one.
- Set up one primary, one alternate, and one virtual command center and make sure each meets the requirements stated in the chapter.
- Make sure your crisis management team has the information it needs and follow the 40-70 Rule in making decisions.

CHAPTER 5: WRITING THE CRISIS MANAGEMENT PLAN DOCUMENT

The heart of any crisis management program is the crisis management plan document. This document pins down in writing the central facts of the plan and guides the crisis management team in responding to an incident.

The written plan sets forth the critical steps of the company's crisis response plan.

It is the playbook the CM team uses to guide it in managing the crisis.

It contains predefined and approved decisions and content to speed execution and management during an event.

In this chapter we'll look at what should and should not be included in a crisis management plan document as well as how a plan document should be formatted and distributed, and the most common mistake people make in writing them.

For convenience, in this chapter when we use the term *crisis management plan* it will refer to the written crisis management plan document.

The Role of the Crisis Management Plan Document

Just as each member of the crisis management team has a role to play, the CM plan document has a role. In fact it has three of them:

- **Program development aid.** The task of writing the plan nudges people toward developing their program and plan.
- **Training aid.** In consulting the plan during training exercises, CM team members gain mastery of the steps of their organization's crisis response.
- **Crisis playbook.** During a crisis, the members of the CM team consult the plan for guidance on what to do. This is its most important role.

Crisis Management Plan Writing Tips

Before we get into the substance of writing the CM plan, here are a few quick tips to help you make sure yours can do the job for which it is intended:

- **Put the content in a logical order.** Put things in the order in which they are likely to come up, as in a story.
- **Go easy on the acronyms and terminology.** You want the document to be readily understandable by everyone who might have to use it.
- **Stick to the essentials.** Reduce the impulse to add fluff. You can't make a CM plan good by making it long. In fact that makes it worse by making the important material harder to find.
- **Use a checklist approach.** Only include the steps a professional would need to be told or reminded of.

A competent CM plan document is feasible and executable. It follows the critical path.

What Does Not Belong in the Crisis Management Plan Document

The most common mistake people make in writing the CM plan is putting things in that don't belong.

Why Including Extraneous Material Is Harmful

Many people assume that including unneeded material in the CM document is not a serious problem. "What's wrong with having extra material in the plan?" they think. "It makes it more comprehensive."

The problem is that having extraneous material interferes with the document's serving its purpose. The CM plan document is not a container for all of the written information that has been produced about your program.

It is a utilitarian, skeletal, front-line document that people will open in a crisis to find out what needs to be done and who should do it.

To put it in everyday language, filling the CM plan full of junk makes it a lot harder to use.

Filling the document with fluff makes it harder for people to find what they need or to notice things that are important.

This results in it taking longer for people to accomplish critical tasks or even in them missing tasks entirely, thus increasing the damage from the crisis and the time to recovery.

The cost of including extraneous material is high, and as a result you should strive to keep such material out your document.

Things to Leave Out of Your Crisis Management Plan Document

What are some of the things that you should not include in your crisis management plan document? Here is a partial list:

- Clip art
- Cartoons
- Audit information
- Policy statements
- Justifications

The CM document should not have any of these things in it because they interfere with its purpose, which is providing clear, easily accessible instructions on what to do to manage an emergency.

What Belongs in the Crisis Management Plan Document?

Having explained what does not belong in the crisis management plan document, we can now look at what does belong.

There is not a one-size-fits-all solution to the problem of how to write the CM plan. This is because every organization is unique in terms of its industry, culture, plan, and priorities.

The information below amounts to suggestions about common elements.

Suggested Organization of Plan Document

There are many ways to organize a CM plan document. A typical and effective method is to divide it into four sections as follows:

- Plan Purpose and Priorities
- Plan Activation
- Event Management
- Appendices

The Event Management section would contain the heart of the document, namely the task checklists for each member of the CM team.

Core Contents of the Crisis Management Plan Document

Every organization's CM plan will be different; however, there are several sections that should have a place in almost every crisis management plan.

Below is a list of those sections in the order in which they commonly appear.

Remember that in every case the information should not be merely explanatory. It should be functional and useful in moving the execution forward.

- **Purpose.** A brief statement of the purpose of the plan.
- **Crisis Management Priorities.** Very important. This is a list of the things the plan is devised to protect. Typically the priorities listed are some version of the following: protecting life safety, stabilizing the incident, protecting and preserving property, and recovering the business.
- **Planning Assumptions.** The assumptions under which the plan is written. Some facilities or scenarios might fall outside the assumptions and necessitate specific callouts.
- **Plan Scope.** Sets forth the facilities and functions that are and are not covered by the plan.
- **Event Response Process Flow.** A section containing a flow chart showing which actions should be taken by which parties after an incident arises. Helps the team execute the plan in a disciplined manner.
- **Event Detection.** Could also be referred to as Plan Triggers. Sets forth what type of occurrences are sufficient to trigger the CM team to start assembling and the command center to be revved up.
- **Event Severity Matrix.** Includes a table laying out various kinds of occurrences that could affect different areas across the organization (life safety, facilities, etc.). Categorizes them on a scale from low priority to high impact and at different levels of seriousness, from Level 1 (least) to Level 4 (most).
- **Plan Activation.** Sets forth who has the authority to activate the plan, pull the team together, and open the command center. Typically includes the head of the company. Should include others as well (e.g., any two CMT members) to ensure there's always someone available who can set the plan in motion.
- **Command Center.** Identifies the primary and alternate physical command centers and the virtual command center. Gives their locations and any special criteria. Provides the conference bridge for the virtual command center. (The physical centers should also have the ability for someone to call in.)
- **Disaster Declaration Criteria.** States what events are sufficient to result in a declaration of a disaster and who has the authority to make the declaration. Specifies the actions that will occur once a disaster is declared.

- **Communication Guidelines.** Details who will handle communicating to internal and external stakeholders and the media and social media about the event. Explains the who, when, and how (e.g., emails, texts, calls, announcement over loudspeaker) of communication across the board. If there's no crisis communications plan, prewritten scripts for foreseeable situations should be included in an appendix.
- **CMT Organizational Structure.** Includes an org chart of the CM team. Indicates who is on the core team (typically, members of such critical departments as finance, human resources, legal, IT, facilities, security, and corporate communications). It also shows who is on the extended team. Members of the extended team are called in on an as-needed basis, depending on the incident. Different organizations will have different departments represented on the core team depending on their industry.
- **CMT Roles and Responsibilities.** The heart of the crisis management plan. Contains detailed checklists of action items for each role. The items specify things the person in that role needs to do or look into. This will take up many pages of the CM plan.

Appendices

The appendices included will vary from organization to organization depending on each one's industry and priorities. Among the appendices commonly worth including in a CM plan are:

- Event Reporting Forms and Incident Action Plan templates for reporting/documenting the event.
- Collection of pre-written communication scripts (if there's no crisis communications plan).
- List of CMT members and alternates with their contact information.
- List of executives and members of the Board of Directors.
- List and maps of the organization's facilities indicating which ones are critical.
- Guidelines for coping with acute staff shortages (such as might be caused by a pandemic).

Crisis Management Team Roles and Responsibilities Checklists

The checklists setting forth the task lists and deliverables for each role on the team might be the most important part of the written plan. The following are some suggestions for creating these checklists.

- Develop a checklist for each department or role on the CM team (have one for the team leader, one for corporate communications, one for finance, and so on).
- Start each list with a brief statement of that department or role's overall responsibilities during a crisis, using a heading such as "Summary of Tasks" and giving two or three bullet points. (Example: the summary of tasks for a finance checklist might include "Managing spending authority and capital expenditures" and "Tracking of funds for business recovery activities.")
- Format the list in table form with the following three column headings: #, Task List and Deliverables, and Completed.
- Further divide the column marked "Completed" into the following three column headings: Yes, No, and N/A.
- List the important tasks that must be done and include any unique, proprietary information that must be known to complete them.
- Do not include basic instructions on tasks every competent professional in the field already knows how to do.
- If appropriate, the list can be subdivided into different sections (for example, the checklist for corporate communications might include sections on internal communications and external communications).

For more information on how to write a good checklist, see Michael Herrera's post "The 4-3-3 Rule for Writing Business Recovery Checklists," at the BCMMETRICS web site.

Sample Checklist

Below is an example checklist showing what the first few steps might look like for the human resources department:

#	Task List and Deliverables	Completed		
		Yes	No	N/A
1.	Identify areas of immediate concern regarding employees and suggest next steps to the CMT Leader.			
2.	Coordinate with Corporate Communications and Legal in all communications to employees.			
3.	Ensure sufficient HR personnel are available at the crisis site to promptly handle employee questions and concerns.			

The checklist would go on for as many steps as necessary to cover the crisis management responsibilities of the HR department's crisis management team representative.

Use and Benefits of the Roles and Responsibilities Checklists

The use of the roles and responsibilities checklists is straightforward. During a crisis, each team member keeps a copy of their list close at hand. The member works through the items on the list, marking them completed, not completed, or not applicable, as appropriate.

The checklist guides their response, encouraging them to focus on taking the specific actions they need to take rather than on the emotion and excitement of the emergency.

We at MHA have seen over and over again how having a checklist to work through can help people get a handle on the performance of a complex series of tasks during times of stress.

The benefits of CM team roles and responsibilities checklists are:

- They tell the crisis management team members exactly what they need to do to fulfill the responsibilities of their role.
- They reduce the chances of important steps being left out in the confusion.
- They reduce the chances that unimportant matters will eat up team members' attention.
- They provide a ready means for tracking what has been done and what needs to be done.
- They provide a quick means for bringing the team leader up to date on the state of affairs in each department.
- They provide a means of documenting the crisis response.

Other Checklists

The use of checklists need not be limited to the ones setting forth the team members' roles and responsibilities.

Checklists on other subjects can be a valuable addition to your written plan.

The following are other areas that lend themselves to being managed through checklists:

- The overall crisis response. The main actions and responsibilities of the response can be set forth in a two-page checklist for inclusion at the very beginning of the plan.
- Special supplies or backup equipment. Checklists can be prepared to ensure that any necessary special supplies and equipment are in place.

Document Logistics

Once your plan is written, you might have questions about such logistical matters as how it should be formatted, stored, and distributed.

Format of the Crisis Management Plan

In today's world, your CM plan must be format-agnostic. The content should be able to flow into any format.

During an event, some people might access the plan via hard copy and others might view it as an electronic copy on their phone or tablet.

Many people think paper is obsolete. It isn't. We recommend that people on the CMT keep paper copies of the plan in their home, car, and office and electronic copies on their laptop and phone.

We also recommend that extra printed copies of the plan be kept in your command centers. Can you imagine a member of the crisis management team arriving at the command center during an event and not bringing a copy of the plan? It happens.

Distributing the Crisis Management Plan

Crisis management plans contain a great deal of confidential information—for example, the private cell phone numbers of top company executives and the board of directors. For this reason, access to your organization's plan should be limited to people on the CMT.

CM team members need total, all-format access. But the plan should not circulate outside that select group.

The Crisis Management Plan Document Is the Linchpin

The crisis management plan document is the linchpin of the CM program. By making sure your CM plan includes the content and sections set forth above, you are on your way to making sure your company can respond in a rational, effective, and focused manner when and if an event occurs.

Takeaways

- People commonly fill their crisis management plan documents with extraneous material, reducing their effectiveness.
- Every CM plan document should include these core contents: plan purpose and priorities, plan activation, event management, and appendices with useful forms, contact lists, and guidelines.
- The heart of the written crisis management plan is the customized checklists listing the roles and responsibilities for the various team members.
- The plan document should be available in multiple formats but also kept secure, to protect the confidential information it contains.

CHAPTER 6: CRISIS COMMUNICATIONS: SHARING INFORMATION, PROTECTING YOUR BRAND

Crisis communications has become an integral part of crisis management. In today's world, how you talk to the outside world about the crisis is as important as how you manage it, especially for prominent organizations.

If you can't communicate effectively with the media and your internal and external stakeholders, you are in a perilous position. This has become more true than ever in the age of social media, when everyone has a bullhorn and every person over the age of twelve has a TV camera in their pocket.

Your crisis management plan must include a crisis communications plan.

Success Is Won in Advance

When it comes to crisis communications, success is achieved in advance. Those who are prepared can make the best of a bad situation. Those who are not ready are likely to compound their problems.

Here are three steps every organization should take during routine periods to ensure they can communicate effectively during an event:

- **Prepare your scripts ahead of time.** These are scripts for the four or five negative events that are most likely to happen in your industry. These will give you a good foundation to work from if and when you need to edit and use them during an incident.
- **Identify and train the right spokespeople.** Make sure you have the right spokespeople identified and prepared before you need someone to field reporters' phone calls or put someone before the cameras.
- **Set up a system for internal communication.** Make sure you know how you're going to communicate with your own people about the crisis, whether it's through an emergency notification system (ENS), email, or social media.

We'll go into more detail on scripts, spokespeople, and internal communication below.

How to Communicate in a Crisis

Over and over again, we have seen how companies facing crisis situations can double their trouble if they botch the communications part of their response. In the modern environment, the math is simple:

1 crisis + bad communication = 2 crises

Messing up on the communications piece can turn a problem into a disaster.

At the same time, companies that communicate quickly and clearly can earn good will from the community even when the larger circumstances are distressing.

We have had a front-row seat to a great deal of corporate crisis communication over the years. During that time, we've formulated four rules regarding how businesses should communicate during an emergency:

1. **Always tell the truth.** When companies own up to their mistakes and take action to prevent the same mistakes from happening again in the future, they invariably come out on top.

2. **Keep it simple.** Telling the truth does not mean telling every last detail you know. Short, simple communications are better than long, overly revealing communications.
3. **Speak through a single voice.** Appoint a single spokesperson to be the face and voice of the company with the media. This person should be someone who is well trained in public and media relations and specifically in crisis communications. Having a single person as the point of contact for the media will ensure a consistent message gets out to all channels.
4. **Use the 5 W's.** The media gets hungry during a crisis involving a prominent organization or one that affects many people. The media wants a specific kind of information: namely the who, when, what, where, and why of the event, as well as the how. Who was involved? What happened? Where did it happen? When did it happen? Why did it happen? How did it happen? If you tailor your communications to answering these questions, you'll help the media do their job quickly and efficiently. This pays dividends by reducing overwrought speculation and earning more even-handed coverage.

Despite our best efforts, sometimes bad things happen to good companies.

When this happens, we can make things worse by responding in a secretive, chaotic manner.

We can contain the damage or even make things better by providing an intelligent, honest, and disciplined response.

The Social Media Challenge

For organizations, social media is the new Wild West. There is no sheriff and vigilante justice is the order of the day.

The bad behavior of one or two employees, amplified through the bullhorns of Twitter, Instagram, and Facebook, can snowball in a way that threatens a brand that took years to build.

Instead of being the community-minded coffee chain or the airline that offers something special in the air, your organization might suddenly become known as the one with the racist managers or that dragged a passenger off an overbooked flight.

Sometimes social media calls attention to behavior that truly is wrong and should be publicized and corrected.

At other times, things blow up on a company for no good reason.

Unfortunately, the internet is a lot like high school: Some people like to get attention by attacking others, and many find it entertaining to gather around and hoot. If the facts get distorted along the way, too bad.

From the viewpoint of business, the rise of social media has created a significant new set of challenges.

It is essential for business continuity and crisis management teams to think about how to protect their brands, along with their more traditional concerns, when writing their business continuity plans.

How to Protect Your Brand

For most companies, their brand is one of their most valuable assets. Although intangible, a brand is as vulnerable to being damaged in a crisis as a building or computer network. Here are seven tips to help you protect your brand in a crisis:

1. **Become brand-aware.** The days when business continuity professionals could leave worrying about the organization's image to the marketing people are over. Your organization's brand is an asset which needs to be protected just like your physical plant and computer networks. In today's environment, anyone involved in crisis management needs to be brand-aware. Learn to think about the potential negative impact of crisis events on the company's brand and image. Take steps ahead of time and during the event to minimize harm to the organization's reputation.

2. **Include brand protection in your crisis management plan.** Procedures to protect your organization's brand and image should be included in your crisis management plan. When there's an incident, you don't want to have to make it up as you go along. The better prepared you are, the better things are likely to go—and the less negative impact you are likely to see.

3. **Devise policies governing staff social media use.** We recommend that only designated individuals be authorized to communicate about the organization on social media. Staff should receive training to ensure they understand their obligations. When employees freelance in commenting on company business in the public square, misinformation multiplies and the message gets muddled. Remember, even if your staff is not posting directly to social media, their communication with family regarding their safety or what is happening may be shared by those family members. It is safe to say that nothing is private anymore.

4. **Keep an ear to the ground.** What you don't know can hurt you. Just because you can't hear them, it doesn't mean they're not talking about you. And that talk can be harmful if it's negative or incorrect chatter about your organization. You might not be on Twitter or Instagram, but many of your customers or potential customers might be. Your organization should come up with a method of keeping track of what is being said about it on social media and traditional media. This monitoring can be done in-house or by independent consultants.

5. **Have help lined up ahead of time.** A crisis is not the time go shopping around for a crisis PR consultant to protect your brand. Establish a relationship with such a firm ahead of time. That way, when trouble strikes, the necessary relationships and arrangements will already be in place. The crisis PR firm can turn immediately to helping your organization protect its good name.

6. **Draft responses for likely problems in advance**. You can't know exactly what unpleasant surprises fate has in store for your organization. You can draft responses for a few of the more likely scenarios ahead of time. Examples of these are situations where: high-ranking employees are accused of misconduct, the organization's products or services are found to have problems, there has been a safety issue or injury, or unhappy customers are making public complaints. Keep these pre-drafted responses with your business continuity plans and use them for guidance in the first moments of responding to the crisis, tailoring the details to match the specific situation. Language that has been carefully crafted and vetted by many eyes is more likely to be judicious and effective than responses thrown together in the heat of the moment. Having prepared responses that model a tone in keeping with the company's core values can make it less likely you will shoot yourself in the foot in responding to a public-relations crisis.

7. **Establish triplines for bringing in outside assistance.** To facilitate sound decision-making during a crisis, it can be good to establish ahead of time when you will reach out to outside consultants for help. Examples of commonly used triplines include: if the crisis moves from being a local matter to a statewide or nationwide matter or if it involves a serious injury or death.

It might be a while before the internet adopts Emily Post's rules of etiquette and the only organizations that take a licking on social media are the ones who deserve it. In the meantime, your organization can increase its ability to protect your brand and image during a crisis by adopting the tips given above.

Takeaways

- ◘ To communicate effectively in a crisis, you should prepare ahead of time by choosing and training your spokespeople, preparing scripts for foreseeable emergencies, and setting up a system for internal communication.
- ◘ In communicating during an incident, organizations should tell the truth, keep it simple, speak through a single voice, and use the 5 W's.
- ◘ Protect your brand during a crisis through awareness, policies, and advance preparation.

CHAPTER 7: THE ALARM SOUNDS: MANAGING A CRISIS EVENT

Sooner or later it will happen if you're in business long enough: your organization will face a serious incident.

A fire, flood, shooting, cyberattack, explosion, sinkhole, scandal, fatal accident, pandemic, or public relations disaster will break out unexpectedly and threaten to engulf the organization.

How well the company gets through will depend in large part on whether it is sufficiently prepared as described in the other chapters of this guide.

In this chapter we'll give you a feel for what it's like to face a crisis at your workplace as a member of a crisis management team. We'll also share some tips on how the CM team can put its preparations and training into effect to ensure the organization's response to the incident is as effective as possible.

We'll also look at how to document a crisis and crisis response and the difference between crisis leadership and crisis management.

The First 24 Hours

The first 24 hours is the critical period when it comes to responding effectively to a crisis. What can your organization's crisis team do to help it "win" this critical period? Read on to learn the who, what, when, where, and why of how companies can successfully manage the first 24 hours of an emergency event.

Chaos vs. Organized Chaos

The difference between the crisis response at an unprepared organization and at a prepared one is the difference between chaos and organized chaos.

The difference between chaos and organized chaos is like the difference between night and day.

Chaos

In a chaotic crisis response, people run around like chickens with their heads cut off. Emotion runs high and few people know what to do. If someone takes the right action at the right time it is by luck. Confusion reigns, and decisions are made and actions taken by whim. There is duplication of effort and omission of effort. Many actions are taken that harm the organization or waste precious time and resources. Many actions that should be taken are completely overlooked. The people involved usually feel helpless, overwhelmed, and even ashamed because they know their coworkers and the organization are depending on them and that they are doing a poor job of managing the event.

Organized Chaos

On the surface organized chaos looks somewhat like chaos. Even in organized chaos, confusion can exist during an incident and emotions can run high. However, if you look closer, there is a striking difference. In organized chaos, the people responsible for managing the event are all focused on doing meaningful tasks. If the situation is confused, people are actively trying to obtain information to clarify it. There is a general sense that everyone knows their responsibilities, has faith in their plan and each other, and is devoted to soldiering through and taking care of business. This may be the best you can hope for during a serious incident, but it is usually enough. It is often the difference between an organization that quickly works through and rebounds from a crisis versus one that is devastated and brutally embarrassed by one.

Crisis Management Priorities

Before we get into the details of managing a crisis event, it's worth recalling what our main priorities are in doing so. In order of importance, they are:

- **Life Safety.** Minimizing the impact on human life. Trying to get or keep everyone safe. Life safety takes precedence over all other concerns.
- **Incident Stabilization.** Stabilizing the situation and preventing further damage.
- **Property Preservation.** Preserving physical equipment, hardware, and the physical premises.
- **Business Restoration.** Getting back to normal operations. Functionally restoring the business in terms of business processes and IT.

Other valid crisis management priorities include protecting the organization's brand, image, finances, and shareholder value.

Execute Your Playbook

Our advice for how to successfully manage a crisis can be boiled down to three words: **execute your playbook.** In other words, follow the plan that the CMT team has already prepared and trained on, as described in the other chapters. That's all there is to it. It's not rocket science. It's following directions.

As stated previously, the heart of the CM plan is the tasks and responsibilities checklists prepared for each role on the crisis management team (team leader, human resources, finance, facilities, security, etc.).

Assuming that your team has previously put together quality checklists for each role, no one has to do a lot of deep thinking when it comes to managing the crisis. **All they have to do is work through their checklists.**

Obstacles to Executing Your Playbook

What can make executing your playbook hard is the high emotion and confusion of the situation, and the gaps where things happen that are seemingly not covered by the plan.

As the old boxer said, "My plan was perfect until the other guy threw his first punch."

Like that boxer's opponent, emergencies punch back.

Being good at managing a crisis comes down to being able execute your playbook under pressure.

Lifecycle of a Crisis

The following is a general description of what the experience of a crisis at an organization is like, as experienced by members of the crisis management team.

Activating the Crisis Management Plan

Depending on the event, it may or may not be necessary to activate the crisis management team. Some emergencies are acute in the moment but don't have a long-term impact (a prank bomb threat, for example). Others can pose a serious threat to the company's survival.

Thinking about this issue can begin during the incident. Evaluate the potential length and scope of the event. Could it significantly disrupt your operations? Was anyone hurt? Will the media be coming?

As you learn what the situation is, consult the CM plan. The CM plan should include criteria outlining when the plan should be invoked. Have you met the criteria? Activate the CMT to help with assessment and planning.

Shifting into Crisis Mode

At the time a crisis strikes an organization, the leader and members of the CMT are likely scattered throughout the company's facilities carrying out their everyday job responsibilities.

There are typically two paths by which the CMT leader and members come to put aside their ordinary responsibilities and shift into crisis management mode.

- They can be contacted by someone else on the team and informed that there is an incident and that the crisis plan has been activated.
- They themselves can activate the plan after learning that a crisis is unfolding, perhaps in collaboration with a fellow team member.

Crisis management team staffers can learn about an incident at their company in many different ways, including:

- Getting a phone call, text, or email about the incident from a fellow team member.
- Being alerted about the event by a non-team member.
- Hearing or seeing something in the media.
- Learning about the incident on social media.
- Hearing gunshots.
- Witnessing an accident.
- Experiencing network or connectivity problems.
- Hearing the sirens of approaching first responders.
- Feeling an earthquake.
- Seeing smoke or fire at a company facility.
- Hearing a fire alarm.

Regardless of how they find out about the incident, once the team member learns the crisis management plan has been activated (or activates it themselves), they should put aside their everyday duties and shift into crisis management mode.

In doing this, the first step is usually to report immediately to the command center, preferably while in possession of their own copy of the CM plan document.

Convening at the Command Center

In the earliest stages of an incident, the core members of the CMT usually gather at the command center, open their crisis management plan documents, and begin working through the checklists relevant to their role. Among the first tasks they will do is try to learn exactly what is going on and what the dangers to the organization are, keeping in mind the priorities of protecting life safety, stabilizing the incident, and preserving property.

Depending on the size and nature of the crisis, members of the extended team might also be asked to report to the command center.

At this time, there can be a great deal of confusion, uncertainty, and stress. Voices can be raised and tempers short. Alternately, things can seem routine at first and only gradually get worse or reveal unexpected losses and dangers.

Keep Calm and Carry On

It is very important at this time for the members of the CMT to demonstrate the proper degree of urgency. They should not be either frantic or complacent. They should remain situationally aware and focus on doing the tasks set forth on their checklists. In other words, "Keep Calm and Carry On," as the British motivational posters put it during World War II.

The Brits of that era were masters of crisis management. In the Battle of Dunkirk in 1940, they rallied a flotilla of fishing boats and pleasure craft to pluck an Allied army of 300,000 off a French beach, preventing their being captured by the Germans. Talk about keeping cool in a crisis.

A common example we see of people not being calm is when they over escalate a crisis to forestall accusations that they underreacted. Individuals insecure enough to do this should probably not be on the team. Good CMT members exercise good common sense and are confident in their judgment.

Modeling and encouraging the proper attitude is one of the main responsibilities of the crisis management team leader.

Different Zones of Activity

A serious incident at a good-size organization encompasses many layers and zones of activity. The members of the CMT will typically be physically situated in the command center, but through their contacts and information-gathering, they will be aware of activities taking place in many different locations.

This is especially true of the CMT leader, whose job includes synthesizing information coming in from all of the different team members and departments.

The following are some of the zones of activity that CMT members might experience or have responsibility for during an emergency:

- The command center
- The physical site of the emergency
- Facilities that are being evacuated
- Safe zones where people are being evacuated to
- Staging, triage, or treatment areas being used by first responders
- Locations where helicopters are landing
- The location cordoned off by the police
- Places where the media are gathered
- Locations were news conferences are being held
- Computer networks and business processes being impacted by the event
- The virtual space in which financial transactions take place
- Social media where the crisis is blowing up

These can be located in one contiguous physical space or in different states or even different countries. Most of them are physical locations but some are virtual ones.

As you can see from this list, managing a serious crisis can be monumentally complicated. This is why having "winging it" as your crisis management strategy is so foolish.

Use the APIE Approach

We've already talked about the importance of crisis management team members' working through their checklists and staying calm. Admittedly, these things are easier said than done, even for trained professionals.

One approach that can help is the APIE approach (pronounced ay-pie). The APIE method is a well-known framework for managing challenging situations. It formalizes a method that many people use naturally in ordinary circumstances, but which they often forget to use during an incident.

APIE stands for:

- Assess the situation
- Plan your response
- Implement your response
- Evaluate your performance

APIE can be used by CMT members while working through their checklists. It provides a further degree of organization to the process, structuring people's thinking, taming their emotions, and increasing their effectiveness.

Watch for Fatigue

In going down the home stretch of managing the crisis, there are a few other things to remember. One is watch for fatigue.

If the crisis is prolonged, the CM team members are going to get tired and become less effective. The responsibility for monitoring this falls primarily to the team leader.

Crisis situations create a lot of adrenaline but they are also tiring.

Ideally, there will be primary and secondary alternates for all of the roles on the CMT. This is your bench. As people start to fade, the leader should pull people in off the bench and send the starters out to rest.

This also goes for the leader him or herself.

Remember Your Values

Another important thing to keep in mind is, remember your values. Don't lose sight of the core principles of the organization in the heat of the moment.

Stress can make people do funny things.

Beware of any short-term gains that might cause long-term regret.

Does your organization pride itself on being honest and transparent? On taking care of its employees? On being good stewards of the environment? You can hang on to those values even while responding effectively to a crisis. You can and you should. You'll thank yourself in the morning.

Documenting the Crisis

Documenting the crisis is an integral part of managing it. There are two aspects of documenting a crisis:

- The front-line CMT members' filling out event reporting forms in real time
- Information from these forms being consolidated and sent up the line to brief the team leader and senior executives

The Importance of Good Crisis Documentation

Good crisis documentation is important for a number of reasons. These include:

- The CMT members' event reporting forms provide the team leader with up-to-the-minute information on what is going on and what actions have been taken in the various crisis management areas. This helps the leader understand the overall situation and coordinate the overall response.
- The information from the event reporting forms might also be used in reports that are sent to senior executives to keep them informed.
- The information is also helpful for any alternates who are brought in to spell the original team members.
- When the crisis is over, the documentation about the event can be used to construct an accurate, detailed timeline of the incident. This helps in identifying the strengths and weaknesses of the CM plan and the CMT's performance. This information can be leveraged to strengthen the program moving forward.
- The documentation can also be important for legal and insurance reasons.

Resistance to Documenting the Crisis

Crisis management team members are typically not very enthusiastic about filling out crisis documentation. Anyone who insists that CMT members keep careful records of their findings and actions is probably going to come in for some grief. Here are a few ways to neutralize this resistance:

- Inform each new member at the time of their proposed induction into the CM team that their core responsibilities include documenting any events they are involved in.
- Make sure documenting the event is an item on each team role's Task List and Deliverables checklist.
- Explain the importance of the team members' event reports to the overall crisis management effort.
- Include filling out event reports as part of any training the team performs.
- Make the event reporting process as clear and simple as possible.

How to Document a Crisis

The following are some suggestions on how to document a crisis:

- Create a simple event reporting form that has places to track the status of the event in the reporter's area, including the issues faced, actions taken, successes achieved, and problems that remain. The form should be self-explanatory, and team members should be trained in its use ahead of time.
- Inform team members that more documentation is better than less.
- Assign one or more people to the task of assembling and summarizing the completed event reporting forms. On a regular schedule (such as every four hours), these team members should produce a rollup report indicating the highest priority issues and give it to the CMT leader. Project management and/or audit personnel are good at performing this role.

- Create ahead of time a form called an Incident Action Plan (IAP) with space to indicate what actions should be taken in the next shift based on the current state of the event (recovery status, people, systems, etc.). Before going off-duty, the team leader should complete a copy of this form to provide guidance for the next shift.
- Also before going off-duty, the CMT leader should use a standardized agenda to brief the team and senior management on open issues for the next operational period (e.g., eight hours). A standardized briefing agenda ensures that key status updates are presented in a consistent manner and minimizes the potential for omissions.
- Once the event is over, a comprehensive after-action report should be written, drawing on the documentation prepared by the team during the event. After-action reports are discussed in the next chapter.

Crisis Management and Crisis Leadership

In the course of handling a crisis, the people in charge of the organization's crisis response will be called on to provide two kinds of direction to those who are depending on them.

These can be described as **crisis management** and **crisis leadership**. The well-prepared CMT should be able to employ both as it navigates an incident. Both are crucial to a successful outcome.

Crisis management is tactical and crisis leadership is strategic. Both are explained in more detail below.

Crisis Management

Crisis management is the task of handling the tactical, short-term aspects of responding to an incident. Most of the sections of this ebook so far have been about aspects of crisis management. Crisis management is concerned with the following:

- Initial Reactions
- Tactical Actions
- Processes

Its horizon is narrow and tightly focused. Crisis management is about working with first responders, relocating staff, dealing with the media, and similar matters.

Crisis Leadership

Crisis leadership is the long-term, high-level component of responding to an incident. Its main concerns are:

- Anticipating the impact of decisions
- Using corporate principles to guide actions

Its focus is wide and its nature strategic. Crisis leadership is about protecting the relationships and reputation the company needs to continue to thrive long-term.

A Shortage of Leadership

We find that most CMTs do reasonably well at crisis management; they can handle the tactical aspects of their role.

But we consistently see a shortage of crisis leadership.

Too often the crisis management team loses sight of the big picture, doing things in the short term that cause harm in the long term. These can include showing disregard for the company's employees, customers, the environment, or core values. Such disregard can damage trust, hurt morale, alienate stakeholders, and tarnish the company's reputation. Such missteps can burden the organization long after the immediate crisis is a memory.

For this reason, we suggest that as part of managing a crisis, the team do a little less managing and a little more leading. The truly successful CMT balances a focus on managing with attention to the larger, strategic concerns that are the focus of crisis leadership.

The Hallmarks of Good Crisis Leadership

The following are some of the hallmarks of good crisis leadership:

- A high degree of compassion and caring for the people impacted by the event.
- The ability to perceive and empathize with employees' stress and their concern for their own and their families' well-being.
- A high degree of emotional maturity and self-regulation.
- The ability to exhibit strength and patience in support of others who are showing the strains of the crisis.
- The ability to balance short-term needs (such as minimizing human impacts and keeping operations running as normally as possible) with long-term ones (such as minimizing brand impact and ensuring customers are not lost due to service impacts).
- Knowledgeable about the organization's stakeholders and their various expectations.
- Sensitive to the context in which the event is occurring (for example, whether your company is the only one affected or one of many, as is often the case in a natural disaster).
- Able to consider the needs both of internal stakeholders (staff) and external ones (customers and vendors).
- Able to grasp the likely limits on external stakeholders' willingness to make allowances for the emergency.
- Able to communicate to stakeholders in a manner that fosters teamwork, gains consensus and buy-in, and facilitates prioritization and executive decision making in a timely manner.

Good crisis leadership is compassionate, mature, wise, and well-informed.

How to Develop Crisis Leadership

The following are some tips to help your organization's crisis management team heighten its crisis leadership skills:

- Use short, 30- to 45-minute mock disaster exercises to educate the team both in crisis management and crisis leadership.
- These exercises should initially require the team to focus on the immediate needs of dealing with the (simulated) event.
- Once the management-level issues have been engaged, the exercise leader should shift the focus toward the higher-level, leadership-type issues.
- The leadership issues addressed might include requiring the team to anticipate the impact of its actions, to use corporate principles to make decisions, and to consider the entire enterprise over the long-term.

The Crisis Ends

Eventually every storm blows out, and every crisis comes to an end. The following are some questions the CMT should start asking as the acute phase of the incident winds down:

- Have we stabilized the event?
- Is everyone safe?
- Does the current status of our people allow the execution of our business continuity and IT/disaster recovery plans?
- Is the organization's property safe?
- Does the current state of the property allow for BC and IT/DR plan execution?

When these questions can be answered in the affirmative, the organization is ready to move on toward restoring its business processes and IT systems—and also toward analyzing the crisis and response with an eye toward learning lessons for the future.

Takeaways

- In dealing with a crisis, it might be that the best you can hope for is to have organized chaos rather than chaos, but this can make all the difference.
- The best way to manage a crisis is for the people on the team to keep calm, remember the CM priorities (protect life safety, stabilize the incident, preserve property, recover the business), work through their checklists, and use the APIE approach (assess, plan, implement, evaluate).
- In handling a crisis, it's important to watch for fatigue, remember your values, keep good documentation, and practice crisis leadership as well as crisis management.

CHAPTER 8: ONCE THE SMOKE CLEARS: MANAGING THE AFTERMATH

Many organizations that are struck by a crisis are surprised to discover that even when the incident is over, it's not really over. It's not unusual for a crisis to have a long afterlife.

Sometimes an event is just a blip. Sometimes it is the beginning of a long road back to normal operations.

The days and weeks after the smoke clears are often the beginning of a long phase in which crisis management is blended with business recovery.

In this chapter, we're going to look at working through the last stage of the crisis management process, including transitioning back to normal operations, coming to grips with your losses, and turning the crisis into a learning opportunity.

Is It Really Over?

The first thing you should do before moving on from the crisis is making sure the crisis is really over. If it is not, you need to continue with implementing your crisis management plan.

As mentioned at the end of the previous chapter, the urgent part of the crisis is over once the following are true:

- Everyone is safe.
- The event is stabilized.
- The organization's property is safe.
- The current status of the organization's people and property allows the execution of the business continuity and IT/disaster recovery plans.

When these things are true, you are ready to move ahead with transitioning toward resuming normal operations.

Many people are surprised to find that the process of grappling with an incident is often more circular than linear. The crisis management team should expect to have to go back and repeat the steps of the CM plan as it works to bring things under control.

Resuming Normal Operations

Sometimes an incident ends right away with a small impact and no long-term consequences. Other times it can be the beginning of a very challenging period as the company struggles to get back to normal operations.

Some events have little to no impact on the company's ability to carry out day-to-day operations. In such cases, getting back to business as usual is straightforward.

Other incidents can cause significant disruptions.

The Business Continuity Team Steps Up

So far we have not talked about the business continuity (BC) team—the unit of the organization responsible for getting the business operations and IT functions back on track after a disruption.

As a crisis tapers off, the CM team typically winds down its activities as the BC team steps up.

It's important for the BC team to be proactive.

If, during the acute phase of the crisis, it begins to look as though the incident will cause a disruption sufficient to warrant invoking the BC plan, the BC team should start pulling out its business continuity and IT/disaster recovery plans and making any other necessary preparations, just to be ready.

Eventually, the organization's leadership must decide whether or not circumstances warrant activating the BC plan. If they do not, the BC members can put their plans away. If they do, the BC team's proactive stance allows it to swing into action as soon as the situation allows. The BC team begins working through its recovery plan, which becomes the new playbook for working through the situation.

Both the crisis management and business continuity plans should include a business resumption plan that has milestones for returning to regular operations (for example, "when 75 percent of the facility is available").

As those milestones are passed, the organization should begin returning to normal operations.

Coming to Grips with Your Losses

Some crises come and go having caused little lasting damage. Others can be very impactful in terms of the losses they bring.

The following are examples of the losses organizations sometimes face after a serious crisis:

- The destruction of important or irreplaceable assets.
- The need to lay off employees as a result of the loss of facilities.
- Damage to the company's reputation.
- The deaths of employees or customers.

Emotions throughout an organization can be intense after a crisis is over, especially if the losses have been substantial.

For the CM team, handling the aftermath of a crisis sometimes includes managing around its emotional impact on the organization.

The following are some things to remember about dealing with loss and emotion after a crisis:

- Don't expect everyone at the company to be a superman or superwoman.
- People respond differently to stress and loss.
- Be prepared to adjust to everyone's differing emotional capabilities.
- In the aftermath of a crisis, people can have a hard time regaining their focus and getting back to work.
- People might benefit from having time to debrief or destress.
- Emotional wounds, like physical ones, take time to heal.
- Even crisis management team members are human and can feel emotionally impacted by what they go through.
- It can help to make counselors available and make it easy for people to talk to them, if they wish.

Learning from the Experience

Many organizations successfully weather a crisis and then drop the ball by not looking back and drawing lessons from it for the future.

In many fields, it's routine to look back at significant past events to learn lessons that can be applied in the future. The Army conducts after-action reports, secret agents get debriefed, and football teams review game film.

However, post-crisis reviews are surprisingly rare at other kinds of organizations.

We recommend that companies that experience a crisis conduct a formal review of the incident after the dust settles, looking at such issues as what the CMT did well, where it stumbled, and whether the event uncovered any gaps in the crisis management plan.

Crisis events, while sometimes traumatic to the organization, also present a golden learning opportunity.

Conducting a Post-Incident Analysis

We specifically recommend that organizations conduct what is known as a Post-Incident Analysis, or PIA.

A PIA is the reconstruction of an incident to assess the chain of events that took place, the methods used to control the incident, and how the actions of your organization as well as those of outside entities such as emergency services and third-party vendors contributed to the eventual outcome.

A PIA is not a forum for criticizing anyone's performance during the incident or second-guessing any actions that were taken.

Benefits of a PIA

Conducting a PIA can bring many benefits to an organization just emerging from a crisis. These include:

- Creating a comprehensive record of the crisis from which the crisis management plan and response can be evaluated.
- Providing an assessment of the communications carried out during the crisis with internal and external stakeholders.
- Supplying an assessment of the organization's safety practices and related procedures.
- Giving an assessment of the training needs for CMT personnel.
- Providing an assessment of the team's working relationships with outside agencies.
- Allowing an assessment of the team's plan, command center strategy, and other arrangements.

The PIA Meeting and Report

What should the PIA meeting and report cover? The following areas should be addressed, at a minimum:

- **Date and time of the incident.**
- **Location of incident.**
- **Type of incident.** Include a brief description of the type of event (fire, flood, workplace violence, power failure, etc.) that required the activation of the crisis management plan.

- **Situation upon activation of the plan.**
- **The final outcome of the incident.** List the extent of damage and impact to business operations. Include personal injuries or casualties if applicable.
- **Strategy.** List the strategies chosen to respond and recover from the crisis. For each strategy, list what the strategy entailed (e.g., close off the building and relocate affected staff) as well as the results of implementing each strategy.
- **Recommendations.** List any recommendations for improvement of the CM plan.
- **Operational successes.**
- **Stakeholder communication.**

Getting the PIA Reviewed and Approved

The final PIA report should be formally reviewed and approved by the appropriate parties to ensure accuracy and comprehensiveness.

Ideally, the PIA should be completed within 14 days of the crisis, while memories are fresh and the needed records and source materials are readily available.

All participants in the analysis process must be truthful and candid in an effort to determine operational or management areas that must be improved.

It is important to remember that the purpose of the PIA report is not to criticize or discipline any person or to second-guess any action taken during the emergency.

The Silver Lining

By conducting a PIA meeting and writing a PIA report as described above, you can identify what you are doing right and also where your crisis response gaps and vulnerabilities lie.

This information can help you improve your crisis management plan and strengthen your team, increasing the resilience of your organization and better-protecting everyone who depends on it.

Takeaways

- You will know the crisis is over when everyone is safe, the event is stabilized, the organization's property is safe, and you're in a position to execute your business continuity and IT/disaster recovery plans.
- As the business continuity team swings into action, the people affected by the crisis will each begin to grapple with what happened in their different ways.
- It's important to conduct a post-incident analysis (PIA) to identify gaps in your crisis response and make improvements (but not to point fingers).

CHAPTER 9: CRISIS MANAGEMENT TRAINING AND EXERCISES: PREPARING YOUR TEAM

So far we've told you what your organization needs to do to structure and staff its crisis management team, develop and write its crisis management plan, and successfully manage a crisis and its aftermath. However, this formula leaves a gap—some would say a large canyon—that we would now like to identify and help you cross.

The gap lies in between creating and writing the plan and successfully managing a crisis.

The fact is, even once your team has developed a plan and written it down, it is still a long way from being able to confidently and skillfully steer the organization through a crisis.

There are two critical tools to help you bridge this gap: training and metrics.

We'll talk about training in this chapter and metrics in the next one.

The Secret to Doing Well

The secret to doing well in a crisis is to train ahead of time. To rely on your team's improvisational brilliance in the heat of a disaster is like playing Russian roulette with your company's future.

Many executives think that practice is for grinds and that star performers do things by the seat of their pants. When it comes to crisis management, this approach is a good way to lose your pants.

Having a strong crisis management training program is essential to your organization's becoming good at responding to emergencies.

The Importance of Training

In an emergency, people don't rise to the level of the crisis, they rise to the level of their training.

There is a common idea that when people face challenges, they have the ability to rise to the occasion. Maybe in some situations that happens, but rising to the occasion in a business crisis is difficult. There are unique aspects to such a crisis that make effective improvising hard to impossible for untrained people. These include high potential costs to inaction or taking the wrong action, uncertainty, high stress, time pressure, strong emotion, and possible casualties.

If you haven't practiced dealing with a crisis, you probably won't know what to do if one comes.

Responding well in a business crisis is not a matter of performing like an action hero. It's a matter of knowing a certain procedure and being able to follow it under pressure.

How to Mismanage a Crisis

Unfortunately, most companies skimp on crisis management training and drills, even many that invest a lot in business continuity. This is like preparing for a marathon by buying new running shoes but not running any training miles.

Under stress, people go back to their old ways of doing things, even when these are counterproductive. Training is how we discipline ourselves to respond in new and better ways.

Common Crisis Management Mistakes

The following are some of the ways we commonly see people mismanaging incidents at their organizations due to insufficient crisis management training:

- One gung-ho person takes over and sidelines everyone else. This person does what they think is best rather than following the CM plan. As a result, many mistakes and omissions are made.
- People focus on tactics at the expense of strategy.
- People forget the crisis management plan priorities and spend precious time working on secondary matters.
- The team loses situational awareness.
- The team doesn't document the information it receives and the actions it takes.

There is a lot of mismanagement when it comes to crisis management. People tend to freak out, even high-level executives. Most people don't have a clue on how to conduct themselves in a crisis at an organization.

The Solution Is Training

There is a simple solution for all of the above problems: training.

It's amazing what happens when you have a team and train them. A well-trained team responds in a lean, systematic way, smoothly addressing priorities in the proper order.

It is true that some people are naturally more comfortable than others in dealing with high-pressure situations. Often such people grow up to become professional first responders. But even first responders train constantly to accustom themselves to operating under stress.

Training can help ordinary people get more comfortable in working under pressure and can increase the chances of their behaving effectively during an incident.

Many people misunderstand the nature of crisis management. It is not about acting like a hero in a movie. It's about calmly following a rational, pre-considered procedure—even when the larger situation is anything but calm.

There is a sure-fire way to raise the ceiling of your company's crisis management performance: having frequent and realistic training sessions.

Mock Disaster Exercises

The secret to performing well in a crisis is practicing ahead of time. How does a company get such practice? By holding mock disaster exercises.

Planning and conducting such exercises is a complex task with many potential pitfalls.

Planning a Mock Disaster Exercise

Here are the 12 steps we suggest companies follow in planning a mock disaster exercise:

1. **Consider the disaster scenarios the team has used in the past, if any.** You will either be devising a new exercise or reusing an old one. You might want to reuse an old exercise if significant gaps were exposed the first time and you want to replay the scenario to assess improvement.
2. **Review action items from any previous exercises, if applicable.** Make sure any outstanding issues have been resolved and will not cause problems for the upcoming exercise.

3. **Consider the maturity of the team.** Less mature teams should be given fairly basic exercises. Mature teams can handle more complex challenges.
4. **Identify the key objectives.** Figure out what you are trying to stress test. Focus on a core set of objectives that you would like the exercise to meet (e.g., reviewing your CM documentation or making sure people are well-trained to perform in their roles). This is an area where less is more.
5. **Identify subject matter experts who can aid you in building the exercise.** Planning a mock disaster exercise is much easier when you have the proper help. SMEs can be from inside or outside the organization or a combination of both. Leverage their expertise to help you build the scenario. Look for people who will help you build a viable scenario rather than simply pick your ideas apart. Avoid consulting people who will be participating in the exercise.
6. **Brainstorm with your SMEs.** Meet with your subject matter experts to develop and refine your scenario. Validate that the exercise framework meets your objectives. Identify and plug gaps in the scenario. Clarify areas that might confuse people. You don't want participants pointing out holes in the scenario.
7. **Keep it real.** The scenario should be a plausible, real-life type of situation. No zombie apocalypses or Marvel superhero attacks. You want people to focus on how to respond, not on the zaniness of the scenario.
8. **Build a timeline and list of events.** In cooperation with your SMEs, work out the details of the exercise, including how much time you will devote to it. Consider the maturity of the team in determining how long you will give them to respond to the events in the exercise.
9. **Build in a Plan B.** When you plan the exercise, have a few different paths ready in terms of how the scenario might go. Sometimes the team makes choices that make the rest of your plan inoperable. Don't force the team to go down a certain path just for the sake of your exercise. Be prepared to adapt to the team's choices. Make sure you can keep feeding the team fresh, relevant problems no matter what choices they make.
10. **Revise the scenario as needed.** Subject the scenario to a process of draft and revision. Work on it over time, adjusting it as people identify areas where it can be improved.
11. **Choose a facilitator.** This is a critical decision. The choice of a facilitator can make or break an exercise. A good facilitator is knowledgeable about the scenario and organization. They are a strong, engaging leader who has the knack of hanging back and letting the team grapple with problems, rather than overdirecting everything.
12. **Consider bringing in outside help.** Still not sure how to proceed? Are you envisioning a large, complex exercise with many phases and participants? Want to make sure your scenario is sufficiently thought-out? If so, you might consider bringing in a business continuity consultant to help. Good advice in the planning stage can be the difference between a successful mock-disaster exercise and one that fizzles out inconclusively.

The key to performing well in a crisis is to train on how to deal with them ahead of time. In business continuity, we do this by conducting mock disaster exercises. By following the 12 steps given above, you can devise an exercise that will realistically challenge your team, improving their ability to respond to a crisis and boosting your company's resiliency.

Exercise Objectives

To be effective, a mock disaster exercise must be designed to accomplish specific objectives. The following are examples of worthwhile disaster exercise goals:

- Transfer knowledge to participants for them to use when a real event occurs.

- Validate the process used by the team to respond to the crisis and resume business operations.
- Validate the CM plan and its capabilities.
- Assess the participants and their capability of following the CM plan and responding to the event.
- Heighten the capability of the team.

Facilitating a Mock Disaster Exercise

Facilitating a mock disaster exercise is a critical, high-pressure task that takes a rare combination of skills. The choice of who will be the facilitator can make or break a mock disaster exercise.

Can a well-planned exercise fall apart if the facilitator is not highly skilled? It happens all the time.

The Role of Facilitator

Mock disaster exercise facilitators have to lead the exercise, but they aren't really the leader. A facilitator who gives too much direction is undercutting the purpose of the exercise. At the same, the facilitator can't be a shrinking violet and let the exercise go in a direction that is irrelevant.

You can think of a good facilitator as being like the referee at a pro basketball game. When they do their job well, the players stay focused, the game seems to flow, and no one notices the ref is there.

A good facilitator frames the exercise and guides the participants, making sure they stay on track. At the same time, the facilitator must hang back and let the participants be the ones who do the work and wrestle with the problems.

The role of the facilitator is to present the exercise scenario to the group, update people as new events occur, and keep things on schedule. The facilitator also provides breaks for participants during the course of the exercise.

The facilitator helps guide the scenario along its logical progression from incident to response to recovery and the resumption of business.

The Qualities of a Good Facilitator

What makes a good mock disaster exercise facilitator? Here are some qualities that most successful facilitators possess:

- Command presence.
- Charisma and enthusiasm.
- Deep knowledge of the scenario.
- Knowledge of the personalities and capabilities of the key participants.
- A willingness to follow the agenda—coupled with the ability to adjust on the fly when needed.
- The ability to engage people and get them communicating with each other.
- A sense of humor.
- The ability to tell when people need a break and the willingness to give it to them.
- The ability to tell the difference between a productive, relevant discussion and a time-wasting, irrelevant discussion.
- The willingness to let good discussions unfold and the ability to cut off or redirect bad ones.

Facilitating the Live Exercise

Eventually the planning comes to an end and it is time to conduct the exercise. The exercise could last ten minutes or it could last five hours.

This is the period when the members of the CM team are presented with the disaster scenario and are trying to think their way through it.

For the facilitator, this is the time when they are in the thick of the action, using their skills and knowledge to steer the exercise and guide the participants while still letting them do the work.

Common Mistakes

Here are two common mistakes facilitators should strive to avoid when facilitating a disaster exercise:

- **Being overly wedded to the scenario.** Developments during the exercise might cut the legs out from under your scenario. If that happens, you have to go with the flow. Reach for your Plan B. What's important at this stage is not making people act out a script. It's adjusting as you go and trying to meet the broad objectives of the exercise.
- **Trying to be "the man."** Being the man in this case means being the one who has all the answers. However, when the facilitator is the man, the participants lose out, because they don't get the chance to try to work the problems of the exercise on their own. This means the organization loses out because the people it will depend on to get it through a real-life crisis are not getting the training they need. If the facilitator is the center of attention, then the exercise is not the center of attention. This is not what you want.

Common Problems in Facilitating a Mock Disaster Exercise

In facilitating a disaster exercise, there are almost always problems of one kind or another.

Here are four common problems to be prepared for, along with suggestions on how to deal with each:

- **Participants criticize the scenario.** No matter how hard you and your subject matter experts work at coming up with a good scenario, there are always participants who say, "That's totally unrealistic. It could never happen. This is a waste of time." This kind of talk can be fatal to the success of an exercise. It must be nipped in the bud. In framing the exercise in the beginning, the facilitator should let everyone know that no matter what they think of the scenario, the scenario itself is not up for discussion. The facilitator could say, "It's similar to a real-life emergency. Even if you think the situation stinks, you have to accept the reality of the situation and work to improve it. That's what it means to be a mature professional. It's the same with this mock disaster scenario. Love it or hate it, you have to deal with it and try to fix it."
- **The participants get too theoretical.** This happens frequently. People spiral off into the stratosphere. They start trying to solve the gaps identified during the exercise, for example. This is not the time for that kind of discussion. This is the time for grappling with the situation presented in the scenario. If theoretical conversations spring up, the facilitator needs to cut them off and redirect everyone's attention to working through the exercise.
- **The participants are not engaged.** People yawn, sit stone-faced, stare at their phones or computers, don't say a word. It happens. Sometimes it helps to direct questions toward different individuals to try to draw them in. If someone's totally ignoring you, working on their laptop the whole time, you could quietly mention to them during a break that you've noticed they're busy and suggest they bow out and send their alternate. This can take guts, but sometimes it's the right thing to do.
- **Other business intrudes.** Sometimes other business intrudes on the exercise. People get pulled away to deal with production or business issues. If this happens, incorporate their unavailability into the exercise. It could happen in a real disaster, too. Tell the others to carry on as best they can without the missing person.

Facilitating a mock disaster exercise is demanding but rewarding. The facilitator plays a critical role in ensuring the organization's staff could respond effectively in the event of a real disaster.

A facilitator needs to be crisp and confident so they can manage the participants and keep things on track. They also have to be willing to hang back so the participants are given the chance to work through the problems of the scenario.

Finally, the facilitator has to be deeply knowledgeable about the scenario but also prepared to depart from it and adapt on the fly as circumstances require.

The World of Micro Mock Disaster Exercises

The typical mock disaster exercise is a complex undertaking that must be planned far in advance and requires a lot of hours from a lot of people. Such full-scale exercises are very important in terms of helping organizations prepare for disasters.

However, full-scale exercises are only one of many types of exercises available to organizations that want to improve their ability to deal with disaster. At the opposite end of the spectrum are micro mock disaster exercises.

What Are Micro Mock Disaster Exercises?

Micro mock disaster exercises are extremely brief disaster exercises that are typically included as agenda items during meetings being held for other reasons. A typical micro exercise lasts about 10 minutes. As everyone is sitting in the meeting, the facilitator sketches out a scenario for the participants and asks them questions about what they would do in that scenario.

The participants think about what they would do and share their responses. These discussions are very informal.

The Benefits of Micro Mock Disaster Exercises

The following are some of the benefits of micro mock disaster exercises:

- They help keep your recovery team personnel sharp.
- They help keep the business continuity process fresh in people's minds.
- They help your team get better at managing the urgent issues that regularly come up in day-to-day business.
- They help your team get better at handling genuine crisis events.
- They help your team develop its crisis management skills and chops.
- They help you make business continuity part of your organization's culture.

Micro Exercise Scenarios

Many different scenarios are appropriate for micro mock disaster exercises. The scenario can either be a small situation looked at in its entirety or a small part of a large situation.

The trick is isolating and identifying challenges whose scope is appropriate for a discussion of 10 minutes or so.

Here are some possible scenarios a company might use for micro mock disaster exercises:

- Tell the participants there has been an outage at your organization. Ask them to find and open their business continuity plans.
- One of your major vendors (specify which) has suffered an outage that will keep them offline for five days. Ask your participants what they will do to minimize the impact of the vendor's outage on your organization.

- Tell the participants they must evacuate the building and will not be able to return for a week. They have three minutes before they must be out the door. Ask them what they can do in that time to minimize the impact of the evacuation on the organization.
- Say that one of the organization's key vendors (specify which) has unexpectedly gone out of business. Ask the participants what they will do in response.
- Tell the participants an active shooting is in progress at one of the company's other locations. Ask them what the initial risks are and what actions they will take.

Conducting a Micro Exercise

The following are some tips for running a micro mock disaster exercise:

- The typical order of business is: present the scenario, have the team address the immediate tactical needs of the situation, have them look at the longer-term issues associated with their decisions.
- Use a timer to keep people focused.
- Document people's answers and ideas.
- Good opportunities for holding micro exercises are during weekly staff meetings, departmental leader meetings, and senior leadership events.
- Managers should then hold exercises with their respective teams.
- Micro mock disaster exercises can be either announced ahead of time or a complete surprise. Generally, exercises should be announced with groups that have little experience in disaster exercises. They can be unannounced for groups with more experience.
- Since micro mock disaster exercises are highly informal, there is usually not any sort of written after action report.
- The BC team should seek and share informal feedback as a way of helping all the parties improve in their roles.
- Test the emergency notification portion of your plan on a monthly or quarterly basis. Do this by sending people a message through your notification system and asking them to reply to you through the system acknowledging receipt.

Establishing a Micro Exercise Program

The first step in establishing an ongoing program of micro mock disaster exercises is obtaining management buy-in. Because micro exercises only take a few minutes and can be slotted into existing meetings, management tends to be more likely to agree to them than to other types of exercises.

To persuade management that micro exercises are worthwhile, tell them about the benefits to the organization's readiness as discussed above. Mention that conducting micro exercises will help with audit and regulatory matters, if applicable.

Once management agrees, a schedule needs to be set up and scenarios devised.

In the beginning, the BC team is likely to facilitate the exercises. Over time, BC staff should shift to observer status allowing the departments to run the exercises themselves.

Full-scale mock disaster exercises are irreplaceable, but a program of micro exercises can bring great benefits at a minimal cost in disruptions. By keeping such exercises short but conducting them often, you can make disaster preparedness part of the culture at your organization.

TAKEAWAYS

- The secret to performing well in a crisis is to conduct realistic training exercises ahead of time.
- Follow the recommended steps for planning a mock disaster exercise.
- The conduct of the facilitator is critical for the success of an exercise; a good facilitator keeps the team focused but lets the members grapple with the problem on their own.
- Conducting frequent micro disaster exercises can help keep your team sharp and make crisis readiness part of your organization's culture.

CHAPTER 10: CRISIS MANAGEMENT METRICS: A TOOL FOR IMPROVEMENT

Along with training, metrics are an invaluable tool for managing and improving crisis management performance.

Regardless of the activity, metrics can help you identify your strengths and weaknesses and the results of your efforts to improve. Metrics drive the control and feedback loop, make the process objective, and are necessary for setting improvement goals.

Metrics in Crisis Management

At first glance, crisis management might seem to be an activity where metrics cannot be used since nothing about it is inherently quantifiable.

In fact there are ways of measuring performance in crisis management.

Such metrics can help your organization identify the strengths, weaknesses, and opportunities of its crisis management posture. They can also help you in creating an optimally performing crisis management team.

The things that matter most in crisis management can be tough to quantify, but there are ways of putting number values on them that can yield meaningful insights into your readiness.

The Role of Judgment

The metrics used in crisis management are not purely objective in the way that miles per hour or temperature are. They require a degree of subjective judgment. Namely, they require that the area being measured be assessed by an observer and assigned a value on a scale.

However, by designing the scales and making your observations carefully you can accumulate valuable and reliable insight into the capabilities of your program and team. These insights can be leveraged to improve your organization's ability to respond to a crisis.

Key Crisis Management Metrics

In this chapter, we're going to look at the four key metrics every organization should gather if they want to bet better at handling events. Those metrics are: threat readiness, team capability, infrastructure readiness, and past performance.

Threat Readiness

Threat Readiness is a measure of how prepared your organization is to handle different threats.

To gauge your threat readiness, you should look at three types of threats, rating your capability to respond to each on a scale of 0 to 100. The three types of threats are:

- **Black swan events.** These are emergencies that are unpredictable and unexpected. They come from outside ordinary experience and are potentially very damaging.
- **Events that are known and prepared for.** These are things everyone is aware could happen and which the organization has taken measures to deal with. Examples might include storms, earthquakes (if you're in a seismic area), cyberattack, terrorist attack, and pandemics.
- **Events that are known but unprepared for.** These are the negative events the organization is aware could happen but which no one has taken steps to deal with. This is usually because the event is found too frightening to contemplate. An example might be the possibility that the organization could simultaneously lose its primary and backup data centers.

As mentioned above, you should rate the organization's ability to respond to each of these three types of threats on a scale of 0 to 100. Assign scores using criteria similar to the following:

- **0** — The organization has done nothing to prepare for this type of threat.
- **1–60** — The organization has taken a few steps toward being prepared.
- **61–80** — Some solid provisions for this type of threat are in place and the organization is making good progress.
- **81–100** — The organization is in pretty good shape in terms of being prepared to deal with this type of threat.

Team Capability

Team Capability is a metric that lets you quantify the skills of the crisis management team leader and members across various areas.

The first step in employing this metric is to make a breakdown of the different skill areas that are most important to crisis response at your organization. Here's an example of such a breakdown:

- **Knowledge of role.** Clearly understands what their role is and isn't. Understands the steps and actions they need to take in their role.
- **Situational awareness.** Maintains a clear picture of what is happening around them at all times and how it will impact them now and in the future.
- **Adaptability.** Able to easily adjust to the new situations and make changes to personnel, procedures, and plans to be successful.
- **Communication skills.** Effectively communicates and collaborates internally and externally as needed in spoken and written form.
- **Self-control.** Able to control emotions and focus on the situation on hand.
- **Ability to think on their feet.** Deals with fluid situations and can devise strategies and plans to deal with a new situation that wasn't planned for.

Next, evaluate how the different CMT members stack up in each area using a scale similar to the following:

- **1 — None/Low.** Little to no experience. Unable to perform.
- **2 — Basic.** Limited ability or knowledge. Needs significant help.
- **3 — Demonstrating.** Able to perform at a basic level.
- **4 — Proficient.** Capable and experienced. Will be Expert with more time.
- **5 — Expert.** Fully capable and experienced. Seen as Subject Matter Expert.

Note that evaluating team members' performance can be a sensitive issue. Most people like to be thought of as being good in a crisis. No one wants to be judged harshly for doing something they have taken on in addition to their regular duties. Emphasize that the ratings aren't an overall judgment on any individual's capability. They measure particular skills that are important in the unique context of crisis management.

This metric identifies how people perform on the unique skills that go toward successfully handling an incident. It recognizes that the skill of the team members and their ability to work together is the main factor in determining how well the organization will respond to a crisis.

Infrastructure Readiness

Infrastructure Readiness is a measure of the adequacy of the various structures and facilities needed to manage a crisis. This includes elements such as your command centers, supplies, virtual meeting bridge, and emergency notification system.

Break down the elements of your infrastructure that are the most important then assign each a score on a scale of 0 to 100 as follows:

- **0** — You have nothing in place.
- **1–60** — You have at least some basic operational capability.
- **61–80** — The core components are present.
- **81–100** — Everything is working normally and you're pretty much there.

Be skeptical. If you set up that conference bridge line for your CMT a year ago, are you sure it still works? Don't give yourself a 100 unless you're sure.

Past Performance

The Past Performance metric indicates how well the team has done in its response to previous incidents, whether exercises or real events.

For this metric, choose five areas that are special priorities for your team and quantify them using a 1-to-5 scale as described above.

Examples of elements you could evaluate include:

- Your ability to notify and assemble the team
- Quality of your command and control
- Whether people understand their roles and responsibilities
- Whether the team can come to a decision quickly

Using Metrics to Improve Your Program

How do you leverage the key crisis management metrics defined above to improve your program? Use them as a guide for focusing your future efforts.

Even informal analyses of the data can pay off in this process. "We're doing well here," you might say. "Let's keep up the good work." Or: "We're really weak here. Maybe we should put a little effort into bringing this area up."

These targeted, rational adjustments will pay off if and when you have an event to deal with.

In addition, you can take the data to your steering committee as a basis for discussions about what new resources you might need.

Dividing your crisis response into different areas and assigning scores to them can provide valuable insight into your organization's readiness to handle whatever craziness might come its way. This approach gives you a rational basis for guiding your efforts moving forward, which is the best way to get the most value out of limited resources.

TAKEAWAYS

- Using metrics can help your organization identify the strengths, weaknesses, and opportunities of its crisis management posture.
- The key crisis management metrics are threat readiness, team capability, infrastructure readiness, and past performance.
- Systematically evaluating where you stand in the key areas gives you a clearer picture of your situation and provides a rational basis for deciding where you should strive to improve.

CHAPTER 11: INTERVIEW WITH A CRISIS MANAGER

In this interview, conducted by MHA staff, **MHA Advisory Consultant Richard Robinson shares his thoughts on crisis management,** drawing on a long career in law enforcement and his experience as one of the first responders at the Sandy Hook Elementary School Shooting

Introducing Rich Robinson

"You're never as ready as you think you are," says Richard Robinson, an MHA consultant who supports security and emergency-related engagements. "When a critical incident occurs, it's never what you prepared for."

Rich should know. He brings 30 years of experience as a security and law enforcement professional to his work as a crisis consultant, including most recently serving as commander of the Technical Services Bureaus for the Newtown Police Department in Connecticut.

As a police officer in Newtown during the Sandy Hook shooting, he activated and opened the town's Emergency Operations Center. After being relieved by the Chief of Police, he was assigned as the supervisor of the Newtown Police Detectives who were working with the Connecticut State Police in investigating the incident.

Since then, he has worked closely with public, private, and parochial schools in Newtown on safety and security issues.

Rich holds a bachelor's degree in justice and law administration from Western Connecticut State University and a master's degree in criminal justice from Columbia Southern University.

Recently, Rich shared some of his thoughts on crisis management, touching on the importance of preparing for the phase after the acute part of the incident, the importance of managing access to the command center, and other topics.

Most Organizations Prefer Wishful Thinking

"Training is beyond crucial," says Rich, when asked what really counts in making an organization crisis ready. "It all comes back to preparation and training."

Unfortunately, he adds, most organizations prefer wishful thinking to investing in crisis management training.

"Most people are unwilling to spend the time and money to do it because they figure it's never going to happen to them," he says.

"The traumatic incident might not, but you are going to have critical incidents no matter how big or small your company is. How well you handle them will be determined by how well you prepared."

Few Teams are Ready for the Second Phase

Most organizations do reasonably well at managing the immediate phase of a crisis but drop the ball after that, Rich says.

"You have to train for an entire critical incident," he explains. "One of the biggest challenges is handling the impact as you segue from the critical incident into recovery."

At Newtown at the time of Sandy Hook, he says, "Our training was for an active shooter but there was nothing beyond that."

This lack of preparation for the period after the most acute phase is common, he adds.

"Most organizations aren't prepared for the second phase, and sometimes the consequences can be life-threatening."

"If you don't have plans to exfiltrate those wounded so you can start doing it right away, you could lose people who could easily be saved," he says. "Ten minutes can mean the difference of someone bleeding out or surviving."

Beyond stopping the immediate source of harm, he says, organizations must have plans for securing the scene, confirming the area is safe, getting EMTs to the victims, treating severe injuries, and removing injured individuals from the red zone.

"You have to plan for the aftermath as well as the emergency," he says. "Most people don't drill to that level. Most people train for imminent threats and overlook the secondary threat."

Have a Single Spokesperson and Pre-written Scripts

Another area where most organizations are underprepared is crisis communications, Rich says.

"Ideally, you should have one person speaking to the media," he says. "If you have to have multiple people from multiple agencies, make sure one message goes out and that one person is creating the message."

"The harm is the media will pick up any nuanced differences and try to eat you up," he explains. "The media if they don't have information, they kind of make it up."

He cites an incident at Sandy Hook where in the early stages of the emergency an unauthorized person gave the media the wrong name for the shooter, causing pain for the families and community.

"It happens in the corporate world, too," he adds. "Even in the corporate world, you can have unauthorized people speak to the media, and they can do incredible damage to the company."

Another point he emphasizes is the importance of having scripts for different eventualities prepared ahead of time.

"Then if something happens," he explains, the spokesperson "just pulls from their list of scripts so they don't have to think about it."

The scripts, Rich says, should address the situations the company is most likely to face, have places to write in the number of casualties, and say something to the effect of, "The company is dealing with the situation, and we'll get back to you with more information as soon as it's available."

"Most organizations aren't prepared well in this area," he says. "Even ones that have practiced, they aren't really good at it."

Keep the Command Center from Becoming a Mob Scene

The management of the command center is another area where Rich finds many organizations are less than prepared.

"If the command center doesn't have a plan for excluding people who don't have critical business there, it creates a mob scene," he says.

"You have so many people trying to get in. Everyone is asking questions. Everyone has an opinion. Some people think they have information that can be helpful."

To allow the crisis management leaders to do their jobs, channels should be established so that people's information is collected and vetted by middle-ranking people then sent up to the top leaders as appropriate.

"Ideally, the command center will have two rooms," he says. "You have an anteroom where you can have meetings with people who have information or updates that need to be given to the ops or finance or logistics leaders. Only have the command staff in the inner area."

He also suggests having the command center segregated from the general public, putting a perimeter around it, stationing an officer or security person at the door, and only letting people in if they have preauthorization.

"This has to be a part of your emergency ops plan," he says. "The plan should say, 'Once a critical incident has been designated and the CM team begins to use the ICS, only the members of the command staff are allowed into the command post.'"

Rich reveals one other measure he has found useful for keeping nonessential people out of the command center:

"We log everyone who goes in and that becomes an official document. We tell them, 'If there's a trial you will get deposed and called as a witness.' That keeps 90 percent of the people out."

The restriction on nonessential personnel should go all the way to the top, he adds.

"This applies even to the CEO," he says. "Put them somewhere else and have them briefed. They aren't part of the decision-making process as you're handling the incident."

The CEO is Probably Not the Right Crisis Leader

Speaking of high-ranking executives, Rich agrees that rank should not be the deciding factor in determining who is in charge during a crisis.

"You don't want to select the incident commander based on their position but on their skillset and knowledge," he says.

In his experience, most organizations get caught up in rank and title when it comes to choosing a crisis leader. He says it's a common belief that to be an incident commander you have to be the CEO.

"In fact," he notes, "the CEO is probably not the right person for that job."

CEOs tend to be strategic thinkers, he says, but crisis management requires a tactical brain.

"The CEO," he suggests, "should delegate to someone who has a better grip of what's going on."

Many Crisis Management Teams Are Confident Because They Are Uninformed

In wrapping up the interview, Rich says that he sees a lot of unjustified self-confidence out there on the part of crisis management teams.

"Everywhere I've been," he says, "no matter how good they think their team was, if you talk to them about incidents they handled, they discover they didn't handle them as well as they thought."

Many people start off by congratulating themselves on how well they managed the crisis, he explains, but as they get debriefed by experts, they come to the realization that there were many CM best practices that they did not know about and did not employ.

If they had used these best practices, Rich says, their confidence would have been more justified and the impact of the incident would have been less.

Takeaways

- It's important to prepare not just for the acute phase of the crisis but for what comes after that; lives can depend on it.
- In managing your crisis communications, it's helpful to use pre-written scripts and critical to have a single spokesperson or at least a single source for information.
- Make sure your crisis plan includes measures to restrict access to your command center to people who have a valid reason for being there.

CONCLUSION

As we said in the beginning, in today's turbulent world, a good crisis management program is a necessity for any organization that wants to be assured of having a flourishing tomorrow.

Trouble can strike at any time, and the best way of making sure your organization can weather a crisis and resume normal operations is to develop a strong crisis management program. This means setting up and implementing a team, plan, and training routine to help you prepare for, navigate, and recover from an incident.

Unfortunately, most organizations are not as prepared as they should be to face a crisis. Do you have a suspicion that this includes the company, nonprofit, or government agency you work for? If so, you are probably right. However, it doesn't have to be this way.

Getting better at crisis management requires neither heroism, genius, or a fortune. All it requires is patiently executing a series of modest, common-sense steps. It's about being prudent and getting ready ahead of time for the storm that will inevitably come.

The gap between where your organization is now and where it needs to be can be crossed. In this ebook, we've tried to show you the steps required to cross it.

As you recall, we concluded each chapter with a list of takeaways to help you get a quick handle on the most critical information.

To conclude the guide as a whole, here is a list of 11 takeaways covering the entire ebook:

- Life is uncertain and the world is becoming more volatile, but you can protect your organization by setting up a sound crisis management program (Chapter 1).
- The way to structure your crisis management team is to have a leader, a core team made up of people from critical departments such as finance, operations, IT, and corporate communications, and an extended team whose members are brought in as needed, with alternates for each role (Chapter 2).
- In staffing a CMT, it is important to choose people based on knowledge, ability, and temperament rather than rank. (Chapter 3).
- Crisis management plans should be simple and robust and establish a primary, alternate, and virtual command center (Chapter 4).
- The heart of the written crisis management plan document should be detailed checklists customized for each role on the team, to guide each person in carrying out their duties (Chapter 5).
- Skillfully managing and sharing information about the incident with stakeholders and the media is a vital part of good crisis management (Chapter 6).
- The best way for the CMT to get through a live crisis event is for everyone on the team to keep calm, remember their crisis management priorities (protect life safety, stabilize the incident, preserve property, recover the business), work through their checklists, and use the APIE approach (assess, plan, implement, evaluate) (Chapter 7).
- When the incident is over, it is important to conduct a post-incident analysis to identify gaps in the crisis response and make improvements for next time (Chapter 8).
- The secret to performing well in a crisis is to conduct realistic, skillfully designed and facilitated training exercises ahead of time (Chapter 9).
- Metrics assessing your organization's threat readiness, CMT capability, infrastructure readiness, and past crisis performance can help strengthen your team and program (Chapter 10).

- It's important to prepare for the period after the acute phase of the emergency as well as to have a single spokesperson, use prewritten scripts, control access to your command center, and staff by ability rather than title, according to law enforcement veteran and MHA Advisory Consultant Rich Robinson (Chapter 11).

Between the two of us, we have around 50 years of experience helping organizations get better at business continuity and crisis management. If you factor in the experience of our colleague Rich Robinson, who provided the material for Chapter 11, our total relevant experience approaches 80 years.

We have enjoyed this opportunity to share some of our ideas and experiences with you.

We tried to treat the topics covered with fullness, but there are limits to what a guide like this can say since every organization is unique in terms of its industry, vulnerabilities, readiness, and culture.

Please don't hesitate to contact us if you would like information on how consulting services from MHA Consulting and software products from BCMMETRICS can help you in strengthening your crisis management program and all other aspects of business continuity and IT/disaster recovery.

Michael Herrera, CEO and
Richard Long, Senior Advisory Consultant
MHA Consulting