CRISIS MANAGEMENT ESSENTIALS

FOR ANY BUSINESS

by : **Cynthia Cavendish-Carey**

Principal Strategist, Strategic Preparedness

Foreword

A crisis is a turning point for a business. It can occur due to an unexpected event, such as an industrial accident, a cyber breach or a pandemic. like COVID-19. It may be the result of something that has been building over time, such as changing market dynamics or new technologies that can kill businesses caught unprepared. At one time, companies like Blockbuster and Kodak were thriving. But not today.

While COVID-19 changed the way many companies do business, you may not be aware that it also drove an increase in cyberattacks ranging from phishing attacks to sophisticated supply chain management attacks that took the digital world by storm.

Since the start of the pandemic, cyberattacks have increased 300% and ransomware attacks cost businesses an estimated $20 billion in 2020. According to a 2021 Threat Report for instance, 11% of manufacturers do not survive a cyber attack.

Regardless of the nature of a crisis, or how it occurs, it frequently requires management to make difficult and critical decisions that could impact the company's future. For this reason, and regardless of your company's size, it is important to have a crisis management plan in place. Having a solid plan in place will not only enable your company to survive whatever comes its way, but you may come out the other side even stronger and more resilient.

Table of Contents

WHAT IS A BUSINESS CRISIS?

Crises happen. That is a simple fact of the business world. To one degree or another, every company will experience potentially debilitating business disruptions. It is not a matter of if a crisis will occur. Rather, it is a matter of when, where, how, and why a crisis will happen, as well as what exactly it will look like and what its impact will be over what period of time. Yet, the ramifications do not have to be devastating provided the proper crisis preparedness planning is in place.

AN OUNCE OF PREVENTION: WORTH A POUND (OR MORE) OF CURE

WHAT IS A BUSINESS CRISIS?

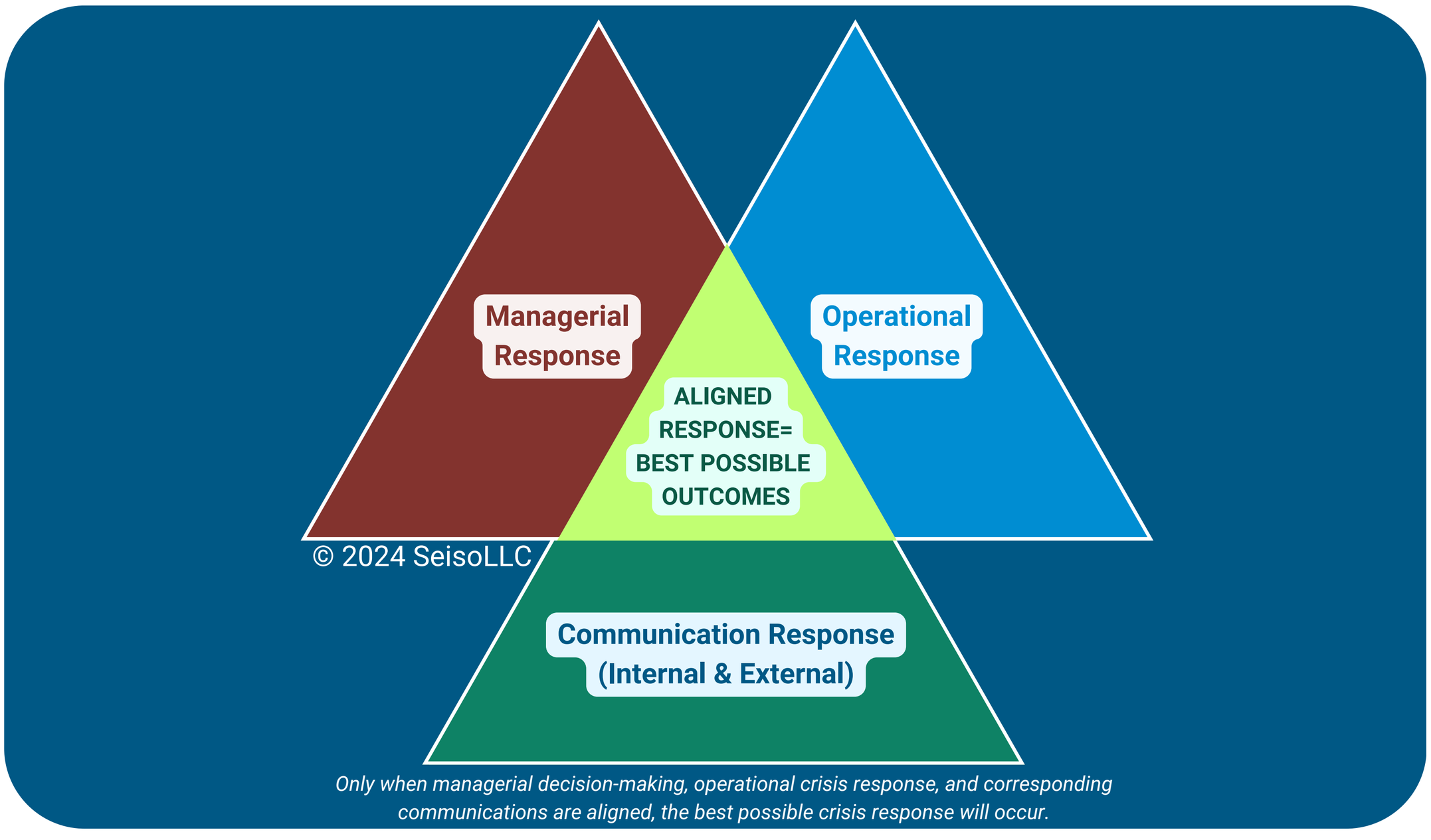
While business crises are typically associated only with negative consequences, most adversarial events and situations can also create business opportunities. In fact, the Chinese word for crisis consists of two characters: “danger” and “change point.” Management should equate the latter with opportunity created through necessary change. There are numerous examples of organizations that have embraced this concept, including during the COVID-19 pandemic. Because many companies were nimble and inventive, they successfully adapted to the rapidly changing business environment. While too often painful to experience, business crises offer opportunities for vital organizational change, renewal, and future growth if management embraces a view from this perspective.

Importantly, research shows that well-prepared companies experience fewer crises and are less likely to suffer significant, lasting damage to reputation, stakeholder trust, and the bottom line. The key lies in thorough crisis preparedness planning, including recurring training and testing of a comprehensive Crisis Management Plan (CMP), that is aimed at optimizing crisis readiness and organizational resilience.

THE FUNDAMENTALS OF CRISIS PREPAREDNESS

The first steps in improving crisis preparedness are to conduct indepth risk and vulnerability assessments and to identify the right employees in the right roles and at the right levels. This requires as well as demonstrates a top-down commitment to helping the company plan for what may come.

The Crisis Response Team (CRT) should be comprised of senior managers representing important functional areas who can lead thoughtful discussions regarding the likelihood of and possible impact from potential crises as well as manage the response to actual crises.



Only when managerial decision-making, operational crisis response, and corresponding communications are aligned, the best possible crisis response will occur.

The first steps in improving crisis preparedness are to conduct indepth risk and vulnerability assessments and to identify the right employees in the right roles and at the right levels. This requires as well as demonstrates a top-down commitment to helping the company plan for what may come.

The Crisis Response Team (CRT) should be comprised of senior managers representing important functional areas who can lead thoughtful discussions regarding the likelihood of and possible impact from potential crises as well as manage the response to actual crises.

Designated employees working in alignment ensures that crisis preparedness planning and crisis response fulfill the company's needs. But this is not a one-and-done proposition. It is essential to view the Crisis Management Plan and its various components as living documents that are never finished and put on a shelf. They must be continually reviewed and refined on a regular basis, as well as in association with real-life adversarial events and situations as part of a robust after-action process.

On the subject of people (and entities), up-front identification of all stakeholders – internal and external – combined with the use of communication channels and tools that are effective and in place for each group will ensure that the organization does not have to scramble during a crisis situation.

Mapping stakeholder groups to communication channels and tools will jump start any response that is required when a negative event occurs. Additionally, communication templates should be part of every organization's Crisis Communication Plan (CCP) and flow into the Crisis Management Plan. The communication templates should be as specific as possible for various scenarios, whether related to business continuity, emergency successions, employee-related situations or legal, regulatory, and legislative issues that might arise. Such templates are fill-in-the-blank but serve at least as a starting point. In the midst of a crisis, CRT members will be grateful to have this support and be able to respond much more quickly than if they had to work from scratch.

Training is absolutely critical to the Crisis Management Plan's and CMP Sub-Plans' efficacy. Educating and training the Crisis Response Team members and their backups regarding where to find and how to use each document, corresponding tools and resources, as well as proper crisis identification, escalation, and notification are essential for enabling an effective crisis response.

Everyone involved in the crisis response must have immediate access to all relevant information at any time, from anywhere. For instance, there are many examples of crises that rendered a facility as inaccessible, plus not all team members are on site especially in today's remote work environment. Even though the CMP and Sub-Plans are confidential and proprietary documents, having hard copies available at all times ensures that no matter what happens with technology, the team can still respond to crises effectively. Through recurring training, each Crisis Response Team member will know where to find and how to access and use the Crisis Management Plan and Sub-Plans, as well as relevant tools and resources.

Additionally, at least annual review and refinement of the CMP will keep protocols fresh, taking into account any new industry or organizational developments, including technological enhancements. Routinely testing specific elements will keep procedures, roles, and the Crisis Management Plan and all Sub-Plans top of mind. Thorough testing and training take any number of forms, including critically important tabletop crisis exercises and crisis drills. Part training, part testing, these drills and exercises must provide safe learning environments designed to help uncover – and remedy – gaps and vulnerabilities in each procedure, role, and crisis response plan. This is a chance for the Crisis Response Team, Subject Matter Experts and backups to detect and solve problems without actually having to act under fire when stress is high.

MANAGING AN EFFECTIVE CRISIS RESPONSE

While business crises occur no matter how much resources companies spend on necessary crisis prevention, there are also different levels of adverse events and situations as well as crisis phases that management must be aware of. First, let us address that there are various levels of business interruptions – not all of which elevate to crisis status.

Adverse events and situations happen at various levels of magnitude and severity, ranging from routine incidents that can be resolved during normal business operation to full-blown crises that require an all-hands-on-deck approach with heavy involvement from the Crisis Response Team.

Phase I: Pre-Crisis Phase

ANTICIPATION

PREVENTION

PREPARATION

Plan the Work

There is a direct correlation between the time and other resources invested in crisis preparedness planning and the company's ability to emerge intact or even stronger from a crisis.

• Assess Risks and Vulnerabilities and conduct detailed Crisis Scenario Planning

• Develop the Crisis Management Plan (CMP), CMP SubPlans, Tools, and a library of relevant resources

• Select Crisis Response Team (CRT) members, Subject Matter Experts (SME), and their backups

• Establish Crisis Response Triggers, Crisis Notification Procedure, and CRT Activation Process

• Conduct recurring Crisis Response Training (Tabletop Crisis Exercises, Crisis Drills, etc.)

• Identify internal and external stakeholders and develop fill-in-the-blank communication templates

• Review and refine plans, procedures, and roles regularly to keep all elements current and useful

• Test the entire crisis response setup regularly with a mind toward continuous improvement

The Crisis Management Plan (CMP), and all Sub-Plans are living documents and should be treated as such.

Phase II: Crisis Response

IDENTIFICATION

ESCALATION

NOTIFICATION

CONTAINMENT

MITIGATION

CONTROL

Work the Plan

When an adverse event or situation does arise — no matter how small or large — the planning, training and testing that have been conducted will help the company to come out on the other side with the best possible outcome. The degree of impact will always depend upon how seriously and diligently preparedness planning during the Pre-Crisis Phase was conducted.

The Crisis Response Phase is all about quickly identifying and accurately assessing the adverse event or situation, proper response team activation and crisis notification, as well as successfully containing, mitigating, and controlling the crisis. The goals are to minimize negative effects, seize opportunities, and bring about the best possible resolution for the company.

The degree of impact on both internal and external stakeholders must be considered as the crisis response unfolds based on plans, procedures, and roles that were determined during the pre-crisis phase. Communication with all relevant stakeholders is exceedingly important — especially if the situation is likely to become public knowledge.

Evaluating outcomes during the Crisis Response Phase is critical and must result in immediate strategic and tactical changes to the response based on the findings.

Include a contingency for an offsite Crisis Command Center (CCC) in the event that all or part of a facility is inaccessible for any period of time. The CCC (onsite and offsite) should be well stocked with predetermined resources including necessary equipment and provisions.

With the proper tools including Crisis Response Logs (CRL) at the team's disposal, appropriate documentation can occur and be utilized in the Post-Crisis Phase.

Phase III: Post-Crisis Phase

RECOVERY

ANALYSIS

EVALUATION

DOCUMENTATION

REFINEMENT

LEARNING

CHANGE

Recovery and Refinement

With careful preparedness and prevention protocols in place, organizations stand their best chance for responding effectively to crises. A completed crisis response, however, is not the time to declare the job as finished. Instead, this is exactly the time to conduct due diligence on what occurred, how well the crisis response was handled, and to apply best practices for moving forward.

Albert Einstein is credited with saying that the definition of insanity is doing the same thing over and over again and expecting a different result. After careful planning and preparedness have been addressed, experience becomes the best teacher. Using a real-life crisis to carefully review, thoroughly educate, and refine procedures, plans, and roles is the wisest course of action.

Postmortem discussions allow all involved team members to bring their perspectives to the table in the interest of continuous improvement. Not an opportunity for finger pointing, this part of the process reinforces the value that every team member brings to bear. Facts and observations should also be documented in an After-Action Report that is preserved. Further, such reports should include the participants' recommendations for improvements to existing plans, operations, communications, etc. In this way, the company is better poised to weather any future crisis.

CRISIS MANAGEMENT BEST PRACTICES

While the number and scope of potential crisis scenarios that are included in the table on the next pages (pages 14-15) may be daunting, the corresponding preparedness planning does not have to be. A streamlined plan that is usable and intuitive can be created to cover all of these situations, including tools and resources delivered in a way that facilitates the Crisis Response Team's and Subject Matter Experts' responses. Leveraging outside expertise to construct a comprehensive Crisis Management Plan (CMP) and related Sub-Plans requires experience that is objective and rooted in a solid track record of helping companies to develop, train, test, and refine it. Trusted external experts can also assist throughout every crisis phase, including with post crisis evaluation that is used for optimizing crisis readiness and organizational resilience.

News channels of every type convey a vast array of crises that occur on a daily basis. Some companies handle these situations well, while others flounder, struggle, and even fight for survival. The difference lies in how well the company prepares, how seriously management takes optimizing crisis readiness, and to what degree this is viewed as part of the culture to employ best practices specifically aimed at crisis management.

Crisis Categories and Triggers

Categories	Triggers
Corporate	• CEO, Executive or Key Employee Emergency Succession (Cause, Demise, or Incapacitation) • Loss of Key Personnel • Travel-Related Accident • Scandal (including Deception, Sexual Harassment or Misconduct, Misappropriation, Misrepresentation, Misconduct, Illegal Actions, Harassment) • Hostage Situation • Leaks of Confidential Information • Lawsuits, Litigation (see also Legal, Regulatory or Legislative Categories and Triggers) • Competitor Hostile Takeovers, Mergers • Market Interference, Impingement from Competitors (Foreign and Domestic) • Negative Industry Publicity (Direct or Indirect/By Association)
Criminal	• Breach, Data Hack or Denial of Service • Viruses, Ransomware • Trade Secret Theft, including IT-Related Events • Acts of Terrorism
Environmental	• Hazardous Materials (Fire, Chemical Spills, Leaks, Toxic Substances) • Any incident that triggers an Insurance Claim
Financial	• Substantial Financial Losses • Substantial Funding Losses (i.e., for Non-Profit Organizations) • Key Customer Account Loss • Losses Resulting from Terrorism
Industrial	• Production Accident Causing Injuries • Any incident that triggers an Insurance Claim
Legal	• Significant Litigation with Claims Asserted Particularly Against Directors, Executives • Allegation of Misleading or Falsified Financial Statement or Other Legal Filing • Class-Action Lawsuit • Scenario Related to Breach of Contract or Other Litigation Event • Other Criminal Activity • Unionization Threat (see also Labor Category and Triggers)
Labor	• Unionization Threat • Medical Emergency (Heart Attacks, Burns, Bone Breaks, Lacerations) • Workplace Accident • Employee Death or Injury, including Murder • Violence or Threats of Violence (including Domestic Violence that could impact the Organization and the Workforce) • Human (Errors, Malevolence) • Rescues • Direct Negative Publicity (Public Demonstrations, Boycotts, Protests) • Indirect Negative Publicity, including Localized, Regional, National or International • Employee or Contractor Strike • Active Shooter Event • Any incident that triggers an Insurance Claim • Fraud (Financial or Other) • Scandal • Illegal Activities • Sexual Harassment or Misconduct • Theft or Embezzlement • Confidential Information Leak (possibly related to an IT Security Event) • Health Threats, including Pandemic Events

Crisis Categories and Triggers

Categories	Triggers
Legislative	• New Law with Significant Negative Business Impact • Sanctions Against Foreign Companies with which the Organization Conducts Business
Natural	• Chronicled (Severe Weather, Tornadoes or Hurricanes, Outages, Geographical, Localized Flooding or Earthquakes) • Infrastructure (Collapse, Equipment Breakage, Fire) • Any incident that triggers an Insurance Claim
Other	• Any Significant Financial Issue with Negative Consequences • Foreign or Domestic Competitor Threats • Product or Component Malfunction • Environmental Release • Client-Related Risk • Key Account Loss • Vendor-Related Issues • Community-Related Events • Negative Publicity for Any Reason
Product	• Malfunction (including Client-Related Issues) • Recall (including Client-Related Issues) • Major Incidents • Planned (Upgrades Gone Awry) • Equipment, Facilities Tampering • Vendor-Related Equipment Failures, Recalls • Vendor-Related IT Security Event • Utility Interruptions • Any incident that triggers an Insurance Claim
Regulatory	• Political Risks • New Laws or Regulations • Negative Impact from Regulatory/Compliance Findings • New Product Requirement • New and Significant Tariffs Imposed or Levied • Regulatory Investigation of Company Officers or Key Employees • Significant Governmental or Non-Government Agency Investigation • Regulatory Enforcement Actions • Inspector General Findings • Fraud Resulting in Meaningful Net Income Loss (possibly related to IT Security, data breach, etc.)
Technological **(See Full List of IT Security Risks)**	• Planned Updates or Upgrades Gone Awry • Data Breach • Denial of Service • Infrastructure • Ransomware • Other

Best practices begin with the company's brand and core values out of which a manageable list of best practices is identified and used as part of the crisis preparedness planning and associated training process. Precisely for any type of organization, the National Institute of Standards and Technology (NIST) is a good resource to compile a customized set of best practices. Using this as a start, here is a recommended best practices list specifically for cybersecurity that according to NIST can also be applied to other adverse situations.

- Maintain human safety
- Maintain environmental safety
- Maintain quality of products, services and operations
- Maintain production goals
- Maintain trade secrets

In addition to NIST's outline and the recommendations included so far, companies do well when management keeps the following in mind and the company utilizes connected best practices.

Expect the unexpected:

enable all employees to identify, report and act quickly to contain and control a wide range of potential adversarial events and situations. This also reduces stress whenever a crisis occurs.

Understand your stakeholders:

know and communicate with internal and external stakeholders in a timely, truthful, consistent, and coordinated manner during all crisis phases.

Ensure top-down leadership commitment:

the tone, tenor, and response begin and end with what comes down from the top of the organization. A C-level champion who oversees crisis preparedness planning, facilitates buy-in across functions, and commits appropriate resources is a must have.

Employees are ambassadors:

every employee – from leadership to the frontline – will be invaluable to bringing a crisis under control as well as communicating with customers, the community, and other critical stakeholders. Cultivating positive relationships will also yield "cosmic credit" when a crisis strikes.

Practice makes perfect:

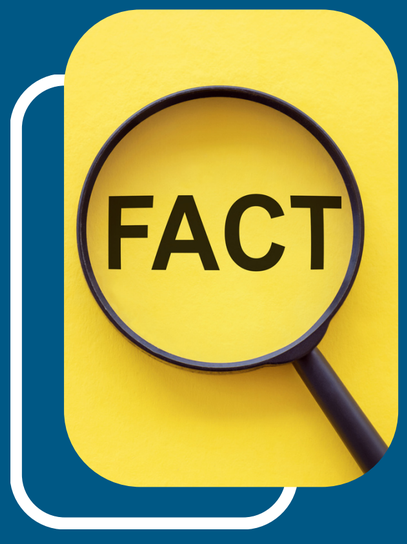
regularly train employees and test the Crisis Management Plan and its components using formal as well as informal tactics, exercises, and drills.

Avoid the blame game:

there is ample time after a crisis is resolved to deal with the repercussions of what transpired. Assigning blame is never appropriate in the midst of a crisis because it sows discord that may lead to delays and confusion when the focus must be on successfully managing the present situation.

One company, one voice:

identify key spokespersons and train them to communicate effectively with key stakeholders such as customers, suppliers, and the media. Unless leadership is involved or implicated, employ a top-down approach to communicating internally. But consider the issue at hand and whether or not it helps or hurts the company and its brand over the long-term to have a CEO publicly out in front.



Be factual and avoid being overly optimistic:

A famous line from Dragnet stated, “Just the facts, ma’am.” It is wise to stick to facts. State only what is known at any given time and offer regular updates to refresh information. Take responsibility that must be taken to avoid becoming a poster child for whatever has occurred. With such an approach, companies can find forgiveness, while otherwise they may become forever tainted.

The end is just the beginning:

once a crisis has passed, it is time to prepare for the future. Debrief, evaluate and ensure that everyone involved has a seat at that table. Lessons learned are a critical part of continuous improvement that helps the organization to identify and better manage risks and vulnerabilities.

Find and leverage the opportunities:

moving beyond a negative event and focusing on a positive direction allows an organization to evolve, renew, and grow. A “what did we learn” attitude and culture instill a constructive optimism in the workforce that encourages team members to propel the company forward and bring about a more crisis-resilient organization.

*More NIST information and resources can be found at https://www.nist.gov, https://www.nist.gov/ and https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf.

IN CONCLUSION

“IT’S FAR BETTER TO PREPARE AND PREVENT THAN TO REPAIR AND REPENT”

Business crises cannot be 100% prevented. Just look at any news channel for proof. It is only through careful planning that crisis readiness and organizational resilience can be assured to the highest degree possible. This crisis management primer offers a thoughtful approach that every organization can put to use.

For any questions and concerns, please call
412.206.6591