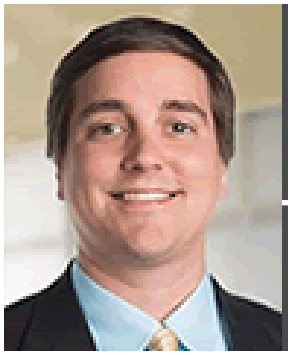


IT WASN'T RAINING WHEN NOAH BUILT THE ARK: EFFECTIVE ELEMENTS OF YOUR DISASTER/CRISIS RESPONSE PLAN

Ray Lewis
Deutsch Kerrigan (New Orleans, LA)
504.593.0697 | rlewis@deutschkerrigan.com

"It Wasn't Raining When Noah Built the Ark" Effective Elements of Your Disaster/Crisis Response Plan
Raymond C. Lewis

We all see in the headlines each day the steady increase in the number and magnitude of disasters and crises that impact companies. Often companies are unprepared and do not have a thorough disaster/crisis plan in place. They believe it will never happen to them. But, what if it does? Benjamin Franklin said it best: "By failing to prepare, you are preparing to fail." If your company lacks a contingency plan that provides continuity or quick recovery in a catastrophic event or crisis, then you, too, are setting your business and potentially your clients up for failure. Before a one strikes, corporate counsel and business owners should think about how a disaster/crisis would impact employees, customers, suppliers, their company's value, and potentially generate litigation.

From weather, fire, utilities outage, human actor, or a security breach, a crisis can strike any company anytime, anywhere. Not having business continuity and disaster/crisis response plan can lead to substantial risks. Depending upon the type of business and particular industry an Emergency Action Plan (EAP) may be required by Occupational Safety and Health Act ("OSHA"). Regulations impacting banks and financial institutions and health care providers either require or strongly suggest that disaster recovery plans be implemented.

An entity's reputation can also take a hit. Clients may accept that an incident happened, but they expect your business to quickly respond. The way an entity responds to a crisis can have a substantial impact on its reputation for years to come. Financial losses may also result from the lack of a disaster or business continuity plan; the longer the downtime, the higher the losses.

Depending on the severity of the incident, your company may also have legal liability that could end up costing even more. Your actions or inactions during an emergency can lead to liability through multiple theories finding legal responsibility. Depending upon the jurisdiction, civil liability grounded in tort is the most likely theory in which liability issues arise in an emergency response. Give the litigious nature of our society, a company should expect lawsuits and claims in the aftermath of a disaster/crisis based on theories of intentional torts, negligence, breach of privacy or confidentiality, premises liability, or medical malpractice.

Notably, tort exposure in disaster and crisis situations is constantly changing. For example, historically, courts have considered the threat created by a mass shooter to be unexpected and remote such that no company should have foreseen the risk and danger.[1] Tragically, as mass shooting incidents become more common, it is possible the foreseeability analysis typically applied by the courts will shift. This shift may have already occurred in Axelrod v. Cinemark Holdings, Inc.[2]—a case that involved the shootings at a movie theater in Aurora, Colorado in July 2012. In Axelrod, the theater's summary judgment was denied on a finding that the plaintiffs had offered enough evidence to create a genuine dispute of fact as to whether the theater knew or should have known of possible security risks. A particular enlightening quote from the

1 See e.g., Lopez v. McDonald's Corp., 193 Cal.App.3d 495 (CA 1987); Sigmund v. Starwood Urban Inv., 475 F. Supp. 2d 36 (D.D.C. 2007); A.H. v. Rocking ham Pub. Co., Inc., 495 S.E.2d 482 (Va. 1998); McKown v. Simon Prop., Grp. Inc., 344 P.3d 661 (Wash. 2015).

2 65 F.Supp.3d 1093 (D. Col. 2014).

Axlerod case suggests that the historical foreseeability bar for these kinds of incidents, which would carry with it possible tort liability, is quickly changing: "what was 'so unlikely to occur within the setting of modern life' as to be unforeseeable in 1984 was not necessarily so unlikely by 2012."

Advanced planning is the key to survival and overcoming adversity and avoiding legal liability. Here are six critical steps to disaster/crisis management that every company should have in place regardless of its size.

Forecast

The first step in any disaster/crises plan should be to predict or forecast the kinds of events that could negatively impact your organization. It is essential to create a set of scenarios that serve to guide planning. This does not have to be an exhaustive list of everything that could happen, but it should represent a broad range of potential emergency situations that the organization could plausibly face. For each scenario or threat you identify, also focus on the potential impact, including: probability the hazard will occur, magnitude/severity of the event, warning time associated with the risk, typical duration of the hazard, and recovery time objectives.

If you can list out your top 5-10 most likely disaster/crisis scenarios, this will go a long way in helping you identifying the aspects of the plan you will need to develop. Some of the issues and hazards to consider when developing your company's plan are:

Geological hazards
- Earthquake
- Tsunami
- Volcano
- Landslide, mudslide, subsidence

Meteorological Hazards
- Flood, flash flood, tidal surge
- Water control structure/dam/levee failure
- Drought
- Snow, ice, hail, sleet, arctic freeze
- Windstorm, tropical cyclone, hurricane, tornado, dust storm
- Extreme temperatures (heat, cold)
- Lightning strikes (wildland fire following)

Biological hazards
- Foodborne illnesses
- Pandemic/Infectious/communicable disease (Avian flu, H1N1, etc.)

Human-caused events
- Product recall
- Management error or omissions
- Hazardous material spill or release
- Nuclear power plant incident (if located in proximity to a nuclear power plant)
- Explosion/Fire
- Transportation accident
- Building/structure collapse
- Entrapment and or rescue (machinery, confined space, high angle, water)
- Transportation Incidents (motor vehicle, railroad, watercraft, aircraft, pipeline)
- Lost person, child abduction, kidnap, extortion, hostage incident, workplace violence
- Demonstrations, civil disturbance
- Bomb threat, suspicious package
- Active shooter
- Terrorism

Technology caused events
- Utility interruption or failure (telecommunications, electrical power, water, gas, steam, HVAC, pollution control system, sewerage system, other critical infrastructure)
- Cyber security (data corruption/theft, loss of electronic data interchange or ecommerce, loss of domain name server, spyware/malware, vulnerability exploitation/botnets/hacking, denial of service)

Use the internet, social media, focus groups, and, if needed, professionals to conduct a business impact analysis to find potential issues that may concern your company. This anticipatory approach should be a regular practice, as should identifying potential scenarios that do not yet exist but could arise because of aspects of your industry.

Prevent

Sometimes, the best defense is a good offense. Every good plan is supported by preventative measures to ensure, as best one can, the scenarios forecasted do not become crises. Identify early warning signs of when an event is maturing or developing into a crisis, develop and implement mitigation strategies tailored to the scenarios you have forecasted or eliminate those scenarios when possible. Get rid of all the low-hanging fruit so your plan can focus on the real disasters and crises.

Position

Not everything is a disaster or crisis nor does it have the potential to escalate to one. Sometimes activating a full-scale crisis response can create an issue out of a scenario that could have been handled discreetly. While

your plan should cover all types of issues and scenarios, your disaster/crisis plan should only be triggered when a scenario escalates to disaster/crisis level. The first part of any adequate plan is to define criteria or benchmarks that provide your team with the information they need to make a determination of when something is or is not a crisis in the heat of the moment.

Sadly, an enormous amount of gray area exists in establishing the tipping point, but some elements you may want to consider are: define what a crisis means whether in the broader sense of the term or by narrowing in and defining certain specific crisis scenarios; internal escalation protocol(s); specific impacts your team should consider when determining the level of an incident; geographic impacts; and whether the issue is attracting traditional media or social media attention. There have to be clear triggers to move the organization from "normal" to "crisis mode" as well as to activate specific responses. Set up a multi-tiered scale, from most to least severe, including trigger points and appropriate actions so that you may properly and swiftly evaluate an incident and act appropriately.

Plan

When the best forecasting and prevention fails, the company must have a plan for dealing with a disaster or crisis. Your action plans are basically a disaster/crisis management check list for your team. They ensure that no important task gets forgotten or overlooked when things get hectic. When creating your action plans, you will want to identify the tasks and action items that each department would need to undertake and accomplish immediately and within the first 24-48 hours of a disaster/crisis occurring. Your action plans can be departmental and should be prioritized in the order you want them completed. Expressly designate an allotted timeframe for completion, try to be as realistic as possible with an understanding of the urgency and hectic nature of the event.

Every plan begins with clear objectives. The objectives during any crisis are to protect any individual (employee or public) who may be endangered by the crisis, keep the key audiences informed, and ensure the company survives. This written plan should include specific actions that will be taken in the event of a crisis. Some of the required elements of a disaster/crisis plan area:

- Includes preparedness and response plans for all relevant emergencies and threats (natural, mechanical, biological, and human);
- Addresses the needs of staff, visitors, structures, and collections;
- Specifies how to protect, evacuate, and recover collections in the event of a disaster;
- Includes evacuation routes and assembly areas for people;
- Assigns individual responsibilities for implementation during emergencies;
- Data and information technologies (IT);
- Lists contact information for relevant emergency and recovery services;
- Includes all needed floorplans, maps, drawings, etc.; and
- Bears date of last revision.

As you develop your crisis management plan, seek advice from the experts that include your leadership team, employees, customers, communications experts, investment bankers, exit planners, lawyers and financial managers. Each of these individuals can provide you valuable insight that could be critical should a crisis strike your company.

Identify chain of command and "owners" of specific tasks.

Crisis demands a fast centralized response and this, in turn, requires a very clear line of command and accountability. A decentralized response is almost always an incoherent response by the organization. The response team should be clearly defined, including backups who would take over if the others were unavailable. You must designate a clear "owner" for each task, preferably someone who is a subject matter expert or holds the most institutional knowledge about that task. Someone needs to own each action plan (for example your department heads may own their respective departmental action plans), as well as each task. Also, create and provide a centralized place for team members to keep notes and document progress for each action item.

If practical and possible, identify the spokesperson that will be the face of the company during the disaster/crisis. If this needs to be a hired public relations professional, so be it. These kinds of situations often require experience in handling the press or local and state officials that the majority of day-to-day employees and officers lack, through no fault of their own. Depending upon the severity or complexity of the situation, there is nothing wrong with getting outside assistance to handle public relations.

Anything you can do beforehand to decrease the risk of scrambling for information while a disaster/crisis is underway will save a lot of headaches during an already stressful time. Make sure contact information of all team members is up-to-date and readily available. Prepare easy to understand checklists of steps of the plan that can be referred to and used by the team.

Communicate with employees, customers, and suppliers.

Who are the people or groups—including the public and the media—related to your company who will need information about a disaster/crisis, and who should information be disseminated to first? When is it appropriate to call in an issue to the C-suite? At what point do you communicate a situation to internal employees and how? These questions should all be answered as part of your plan.

Let employees know where to go in case of disaster or emergency; have a clearly defined backup worksite. Maintaining an informed workforce helps ensure that business continues to flow as smoothly as possible. It also minimizes the internal rumor mill that may lead to employees posting false reports on social media. Easily activated channels for reaching people on site and outside should be utilized. For example, use of text messaging, emergency telephone calls, internal speakers, and TV monitors to make announcements. A shooter on site, for example, triggers facility lockdown and police response but also rapid announcement that everyone should stay where they are, lock doors, hide, etc. To the extent possible there should be redundancy in these channels including backups that are not linked to the telephone system or the Web and the messages should be composed in advance.

The last thing you want is for your customers and suppliers to learn about your disaster/crisis through the media. Information on any crisis pertaining to your organization should come from you first. Part of the crisis communications plan must include the customers and suppliers to notify and how they will be regularly updated during the event. Remember that once the situation returns to normal, you will want to immediately let those same customers and suppliers know you have return to operation. Lastly, make sure your service agreements include clauses that cover disasters/emergencies and define level of service in the event of a disaster.

Pre-approved crisis communication strategy and messaging.

When a disaster/crisis strikes, respond immediately. Have the spokesperson prepared and ready to go. The first few hours are most important in establishing credibility and building public trust and believability. Do not stonewall. Be responsive to the media and inform the people who need to be kept informed, especially employees, shareholders, vendors and customers. Forget the safety blanket of “No comment.” One way or the other, the media will get information, but it may be inaccurate and the sources unreliable. In a crisis, perception is stronger than reality and emotion stronger than fact. As Michael J. Fox’s character correctly noted in The American President: “[I]n the absence of genuine leadership, they’ll listen to anyone who steps up to the microphone. They want leadership. They’re so thirsty for it they’ll crawl through the desert toward a mirage, and when they discover there’s no water, they’ll drink the sand.” Nothing generates more negative media coverage than a lack of honesty and transparency. Therefore, being as open and transparent as possible can help stop rumors and defuse the situation. This transparency must be projected through all communications channels: news interviews, social media, internal announcements, etc. When those responsible do not communicate, the crisis still gets played out in the media and possibly even later in court.

Another secret to successful crisis management is pre-set responses. Timely, consistent and effective communications are critical but quick approvals of communications can be a difficult task. One of your goals should be to pre-define your communications strategy, and to draft your communications and have them pre-approved by all the right members of your team – to the most extent possible. The list of pre-approved communications should include: common talking points/ message points, general communications to employees, communications to clients and suppliers, frequently asked questions (FAQ), preliminary media responses, and responses to local, state, and federal agencies and regulatory bodies.

Leaders should be able to pull combinations of pre-set response “components” off the shelf. Pre-drafting the elements of a crisis response plan provides the organization with speed and uniformity but also flexibility to deal with unexpected scenarios or combinations of scenarios. This is important because real crises rarely directly match planning scenarios. If response options are not flexible, novel events or combinations of events can result in ineffective responses. Response components might include: facility lockdown, police or fire response, evacuation, isolation (preventing people from entering facilities), medical containment (response to significant epidemic), grief management, as well as external communication to media. Matching these components to scenarios enables a response that immediately triggers and accomplishes aspects of the plan. For example, a “shooter on site” event triggers an immediate facility lockdown plus a police response plus preset communication protocols to convene the crisis-response team and warn staff.

While this can often be counterintuitive, it is better to over-communicate than to allow rumors to fill the void.

Issue summary statements, updated action plans and new developments as early and as often as possible. With today's social media and cable news outlets, we live in a time of the 24/7 news cycle. Your crisis plan and communications are expected to and must do the same. Be sure to establish a social media team to monitor, post, and react to social media activity throughout the crisis.

Elements to incorporate into the IT portion of the plan.

Every good, modern-day disaster/crisis plan must include a focus on information technologies and the data your company needs up and running during and after a disaster/crisis. Start by taking inventory of what you have, where it is located, how it is set up, and how vital it is to your operations. A listing and location of any IT resources to be tapped is necessary. Agreements should also be negotiated with external agencies to provide specific resources in time of crisis.

As you create your plan, you will need to explore exactly what your business requires in order to run. You need to understand exactly what your organization needs operationally, financially, with regard to supplies, and with communications. You need to know (1) what you need to restore or initiate to have data services, (2) how long it will take, and (3) who performs each task. Whether you are a large business that needs to fulfill shipments and communicate with customers or a small business to business organization with multiple employees, you should document what your needs are and rank them in order of importance so that you can make the plans for backup, business continuity, and have a full understanding of the needs and logistics surrounding those plans.

Make sure that your data backup is running and include running an additional full local backup on all servers and data in your disaster preparation plan. Run them as far in advance as possible and make sure that they are backed up to a location that will not be impacted by the disaster. If possible, it is also prudent to place that backup on an external hard drive that you can take with you offsite or one that is stored offsite.

Miscellaneous details and objectives.

Other critical aspects of your company plan that should be covered or considered are:

- Plan for your equipment – For geological or weather-related disasters, it is important to plan how to best protect your equipment. For example, in flooding or hurricanes, you will need to get all equipment off the floor, moved into a room with no windows and wrapped securely in plastic so ensure that no water can get to the equipment.
- Detailed asset inventory – In your plan, you should have a detailed inventory of workstations, their components, servers, printers, scanners, phones, tablets and other technologies that you and your employees use on a daily basis. This will give you a quick reference for insurance claims after a major disaster by providing your adjuster with a simple list (with photos) of any inventory you have.
- Command Post – This should be a location that can be rapidly converted to be used by the crisis response team. Requirements include the ability to rapidly connect many lines of communication, to have access to external media (TV coverage), to provide access to crisis management plans, etc. In addition, there should be a backup command post located off-site in the event that evacuation is necessary. This could be located at a home or other location, so long as the necessary IT exists or can be swiftly put in place for communication and other resources.

An electronic copy of this plan should be stored on a secure and accessible website that would allow team member access even when company servers are down. It is also a good idea to provide a copy of the plan to the local law enforcement and public emergency services that would respond to your facility and others with responsibility for building management and security.

Train

The best plans are worthless if they exist only on paper. There needs to be regular, at least biannual, exercises conducted by the crisis response team, and regular testing of channels, inventorying of resources, etc. These tests should be done regularly, but not scheduled in order to test speed of response.

Training personnel so they are familiar with detection, duties, processes, communications, and warnings is vital. Review plans with staff to ensure they are familiar with their role and can carry out assigned responsibilities. Make sure training occurs within the entire team any time one its critical members or leaders is changes or when someone leaves the company. Do new employees know about the plan and what it entails? What about remote employees? Are they adequately identified, aware and informed? As a guide, general training for employees must cover: individual roles and responsibilities; threats, hazards, and protective actions; notification, warning, and communications procedures; means for locating family members in an emergency; emergency response procedures; evacuation, shelter, and accountability procedures; location and use of common emergency equipment; and emergency shutdown procedures.

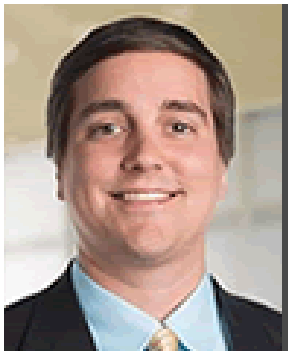
Conduct evacuation, sheltering, sheltering-in-place, and lockdown drills so employees will recognize the sound used to warn them and they will know what to do. Facilitate real world exercises and simulations to practice the plan, familiarize personnel with the plan, and identify any gaps or deficiencies in the plan.

Evaluate

Each crisis provides an opportunity for organizational learning to occur and plans to be revised. After each and every crisis, review the company's performance and focus on continuous improvement. Thoroughly and critically assess how each individual performed and how each layer or level of the plan was implemented and appropriately tailored to the particular crises. Identify where improvements can be made and identify what aspects need further training. The guiding questions should be: What went well and what went poorly? What are the key lessons learned? What changes do we need to make to our organization, procedures, and support resources? Whether your plan was a success can be judged through a number of considerations: (1) protection of your employees, customers, and the public; (2) protection of your reputation and brands; (3) protection of your market share and profitability; (4) reduction of financial loss and litigation exposure; (5) continuation of a commercially viable business; and (6) compliance with all the relevant government and legal requirements.

Do not miss the opportunity to learn from others' successes and failures. Take notice of how other businesses respond to crises or disasters. When the response is a positive example, reach out to the principals of that business and exchange information and ideas. Learn what they did right (or wrong). Determine if anything learned in their experience can be implemented or added to your company's plan. Perhaps they learned along the way that parts of their plan were useless given the realities they were facing. If your plan has similar features, reassess and rethink about changes you may make based on their experience.

There will be little-to-no time for planning and strategizing as a disaster/crisis unfolds. An unplanned disaster/crisis throws a company into panic and survival mode. A disaster/crisis that is not managed well can wipe out decades of hard work and company value in a matter of hours. A well-managed disaster/crisis confirms that your company has the processes and procedures in place to address almost any issue that may develop. The absolute first step towards managing the unexpected situation is to have an organized, well-thought out disaster/crisis plan in place long before your company is faced with adversity.



RAYMOND C. LEWIS

Partner

DEUTSCH KERRIGAN (New Orleans, LA)

504.593.0697 | rlewis@deutschkerrigan.com

Raymond C. Lewis knows that an attorney with courtroom experience is a valuable asset to a client and has developed the skills necessary to get through the unexpected hurdles of a courtroom.

His practice centers primarily in the areas of complex commercial and business litigation, insurance defense, and appellate work. He has successfully litigated complex commercial disputes for local and national clients involving multi-million dollar claims for breach of contract, product liability, oil and gas disputes, and transportation casualty. In his appellate practice, Ray has handled numerous appeals before the Louisiana Supreme Court, Circuit Courts of Appeals, and the U.S. Fifth Circuit, many resulting in published decisions favorable to his clients.

Ray has appeared multiple times as a “Ones to Watch” in the legal industry by New Orleans CityBusiness. He has also been voted to the Louisiana Super Lawyers “Rising Star” List, 2014-2017. He has written and lectured on trial and appellate practice and environmental law topics.

Practices
- Appellate Litigation
- Commercial Litigation
- Commercial Transportation
- Insurance Coverage
- Manufacturer’s Liability and Products Liability

Industries
- Transportation
- Insurance
- Manufacturing

Sucesses
- Robert Sensat v. R360 Environmental Solutions, et al., 31st Jud. Dist. Ct., Parish of Jefferson Davis, NO. C-24-13
- Matrimonial Regimes – Termination of Community
- Johnson v. Transwood Inc., Tuthill Corp., et al, No. 14-102 (M.D. LA)
- Solstice v. OBES, Inc., et al., U.S. EDLA No. 12-2417.
- Construction Defect - Salinger v. Diamond B Construction
- Premises Liability - Miles v. City of Kenner, et al.
- Insurance Coverage - Summary Judgement

Accolades
- The Best Lawyers in America©, 2019-2020
- New Orleans CityBusiness Ones to Watch: Law, 2015, 2017
- Louisiana Rising Stars List, 2014-2019

Education
- J.D., B.C.L., Louisiana State University, 2007
- B.A., Baylor University, 2004