



## DISASTER RECOVERY & BUSINESS CONTINUITY

### DEFINITIONS

Critical Incident: An unanticipated occurrence that causes destruction, loss, or distress to an organization, including natural disasters, technological accidents, or human-caused events, that may result in significant asset loss or damage, multiple injuries or death. a.k.a., “disaster” or “business interruption”

Crisis: any natural or human-caused event (whether accidental or intentional) that runs the risk of (1) escalating in intensity, (2) adversely impacting shareholder value or the organization’s financial position, (3) causing harm to people or damage to property or the environment, (4) falling under close media or government scrutiny, (5) interfering with normal operations and wasting significant management time and/or financial resources, (6) adversely affecting employee morale, or (7) jeopardizing the organization’s reputation, products, or officers, and therefore negatively impacting its future.

Crisis Management: intervention and coordination by individuals or teams before, during and after an event to resolve the crisis, minimize loss, and otherwise protect the organization. This is often done through the development of the Crisis Management or Business Continuity Plan. This includes the immediate intervention taken by the organization to minimize further losses brought on by a critical incident and to begin the process of recovery, including activities and programs designed to restore critical business functions and return the organization to an acceptable condition.

### SIMPLE THINGS TO DO TO KEEP YOUR BUSINESS HUMMING

For obvious reasons, crises are something no one likes to think about. Much as we hope they won’t happen, and especially not to us, history shows the odds are too high to ignore that some sort of crisis may touch us directly or indirectly. The LaSalle Bank fire earlier this month is an in-your-face reminder that “stuff” happens!

No matter what your organization does or what size it is, crisis management matters to you. The four most important assets for an organization are its people, intellectual property, facilities and reputation. How do you protect each of these assets? Which is most important to you? Which cannot be replaced if lost? If you are in an accounting, law or consulting firm, you are in an information processing business. To stay in the game, your business needs to operate effectively and continuously, sometimes 24 hours a day, in order to serve your clients, maintain your internal systems or preserve your data. Consequently, crisis management is a major strategic initiative for most organizations.

Failure to recover from a crisis has led to the demise of many organizations. 43% of businesses that suffer a disaster never reopen. This is a blended number, encompassing very large to small businesses. The smaller the business, the more likely it will cease to exist after a disaster. That’s why companies take crisis management so seriously – and why a crisis management plan is so critical.

Critical incidents can happen at any time to any organization. From major viruses that damage your hardware, software and data to critical employees walking out of the job, crises are to be expected. Your organization must be ready to handle just about every contingency, including the worst of catastrophes. The question every senior executive asks is, “How can we fully prepare for crises when there is no way to anticipate every situation?” Oddly, just because you can’t anticipate everything doesn’t mean you can’t prepare for it. The companies in the World Trade Center never dreamed airplanes would be turned into



bombs, yet a vast majority of them were able to start over because they were prepared for the “worst” – whatever that meant. And remember, insurance is the contingency plan of last resort – it cannot replace what is truly lost.

The best answer is to act like a boy scout – *be prepared!* You must have a clear plan in place to both prevent a critical incident from happening, and to recover within an acceptable timeframe when the unpreventable happens. A critical incident can be any kind of interruption – such as software malfunction, virus attack, database corruption, accidental file deletion, workplace violence, a fire, utility blackout, employee strike, product recall, executive death, intellectual property theft, denial of access to a facility due to someone else’s disaster, or sabotage – just to name a few. Sometimes it is not always a clear line between an event that would be called a crisis and a similar event that is merely an inconvenience. If a complete collapse of a building with a loss of life is a disaster, what about a partial collapse without a loss of life? A partial collapse of a research lab could mean the end to a whole life’s work. That is also a disaster. The challenge facing most organizations is how to minimize the lost revenue and operating expenses these incidents cause. Even without losing people, buildings and equipment to disasters, organizations suffer in many ways, including:

- Loss of employee productivity
- Loss of customer business during downtime
- Loss of customers who, when unable to do business with you, find another vendor – permanently
- Financial penalties from violation of legal requirements

Business recovery depends completely on what you do before the critical incident hits you. Being prepared does not just happen; it takes planning. If Noah had waited for it to start raining before building the Ark, would the animals have been saved? Do you have the proper plans and processes in place?

Your goal is to protect personnel (employees and clients), intellectual property (client files and business data), physical facilities (office and equipment) and your reputation (your good name) from perils which could cause the possible demise of your business. Listed below are some simple steps you can take to help you reach your goal:

- Assign someone in your organization the responsibility of creating and maintaining a crisis management plan.
- Conduct a risk assessment. Survey your building and its environment for security holes and other risks. Survey your business for single points of failure.
- Conduct a business impact analysis. Understand your processes, computerized or not. Where does your revenue stream start? How long can your business operations be down before it causes serious problems (this is your recovery time objective)? How much data can you lose (this is your recovery point objective)? What are the financial, operational and legal impacts of downtime over several timeframes?
- Create an Emergency Response Team and procedures for them to follow and keep these as part of your office manual.
- Create other teams, depending on the size and complexity of your business (e.g., damage assessment team, office services team, departmental teams, etc.)
- Maintain a telephone tree in order to contact staff if a crisis happens outside normal working hours.
- Maintain a current list of client telephone numbers and keep these off site, or easily available via web access to your systems (particularly if your systems are maintained offsite by a third party).



- Review and test your evacuation plan to ensure staff safety and assign someone to assist others who may need assistance in the event of an emergency. Be sure your safety notices are posted in appropriate places.
- Designate a location outside your building as a meeting spot in case of evacuation for purposes of doing a head count.
- Install an automatic fire detection system and an automatic fire extinguishing system. (This could have saved LaSalle Bank from losing an entire floor to fire.)
- Train all your staff about emergency response responsibilities. Every employee needs to know the use and location of fire alarms, fire extinguishers, and evacuation routes.
- Know the name and contact information of at least one crisis professional to assist after the crisis with emotional trauma.
- Establish security procedures and processes and follow them! (e.g., ensure that all electrical devices are turned off when not in use - coffee pots, computers, etc.)
- Gather the following information and keep a copy at the office and at the home of the person responsible for the crisis management plan:
  - Your crisis management plan – which is a step-by-step action plan that is used throughout the response and recovery processes
  - Building management key personnel contact numbers (work, mobile and home)
  - Vendor contact list (including your insurance broker, accountant, legal advisor, and be sure to include vendors who can help in recovering from the crisis)
  - Petty cash and credit card
  - Copies of insurance policies with information about coverage
  - Office lease
  - Client contact information (work and one emergency number)
  - Floor plans
  - Master docket/calendar, if appropriate
  - Client file index and offsite storage index
  - Safe deposit key(s)
  - Banking account numbers

### **Author Bio**

Irene Rozansky is the founder and CEO of Rozansky & Associates LLC, a firm dedicated to helping companies build smarter, stronger organizations that can rebound efficiently from any emergency, ensuring the longevity of their critical business processes. Irene is an international speaker, author and consultant with an extensive background in strategic planning, business operations, business continuity, and organizational change and communications. For more than a decade, Irene has worked with disasters first-hand, and has assisted more than 50 Fortune 1000 companies prepare for, mitigate, and successfully avoid and/or recover from unplanned events. Before forming her own company, Ms. Rozansky was responsible for developing, implementing and managing business continuity consulting services for Digital Equipment Corporation, Compaq Computer Corporation and Comdisco, Inc. Ms. Rozansky maintains a partnership relationship with Apogee Strategies on Disaster Recovery and Business Continuity projects.