

Staying Afloat - Discovering and Dealing with Risks

By Irene Rozansky, Founder/CEO R&A Crisis Management Services



SIGN INSIDE OF LIFEBOAT: *"Some wetness is normal. If submersion occurs, move arms in a swimming motion."*

It's a no-brainer: conducting business-as-usual is extremely difficult when your business is sinking from the iceberg that seemingly appeared out of nowhere. The purpose of contingency planning is to create buoyancy. Bounce back quickly when bad things happen!

One of the first steps in creating a buoyant organization is to discover what you are up against - what "icebergs" are in your path that need to be dealt with from pre- to post-crisis.

No matter how well organized and in control you may feel about your day-to-day tasks, it is impossible to live without risk. Therefore it is imperative that organizations wrap themselves around concepts concerning risk. Amazingly, most organizations do not do this, or don't do a very good job of it.

Start with understanding risk. The components of risk include; a) a potential precarious or hazardous condition, b) an indication of impending danger or harm regarding the condition, a.k.a. "threat", c) an uncertainty about the threat's likely occurrence, d) the difficulty to detect the threat far enough ahead to protect oneself, and e) the vulnerability or impact to the entity should the condition occur.

Risk is *not* the threat itself, which many people often confuse it with. Threat is merely a component of risk. Threats come in a myriad of forms; extreme weather, earthquake, volcano, power failure, single-point-of-failure, computer failure, mechanical failure, workplace violence, ethical misconduct, sabotage, civil unrest (including terrorism), data corruption or looting, malware, flu pandemic, hazardous materials, etc. Some of these threats are under your control, others are not. Some of these threats give off advance warning signals, others do not. Some of these threats are location-specific, such as earthquakes and volcanoes. Some will have greater or lesser impacts to your bottom line, business operations, or reputation, depending on how and when they happen.

To find your most compelling risks, start by conducting an assessment on all possible known threats to your core business processes and facility. But, don't neglect the second-order effects from the risks, too. For example, during Hurricane Andrew, telephone companies discovered that one of the principle shortage was not poles, wires, or switches, it was day care centers. Field

operations employees could not come back to work because they relied on day care, which was unavailable due to the hurricane.

You also need to assess the risks associated with your business continuity plan, assuming one is developed. People need resources to carry out the requirements of the plan. Are they readily available? Have the team members been properly trained to carry out their response and recovery duties? Do you have viable inter-departmental coordination? Are there multiple ways to communicate during a disaster? *Risk Assessments* ask a LOT of questions. They can be tedious, time-consuming and tiring. They can be risky endeavors all by themselves if not handled properly. But best of all, risk assessments unceremoniously expose the icebergs!

Risk value is a measure of the adverse effect of a threat. It looks something like this:

$$\text{LIKELIHOOD} \times \text{DETECTION} \times \text{IMPACT} = \text{RISK VALUE}$$

Once you know the risk values for all your true threats, they can be prioritized by likely impact on the bottom line (or other criteria) and strategies can be developed a) to prevent the threat from occurring, or b) to mitigate the likelihood and impact, or c) to simply control the outcome. Keep in mind, risk assessments are more art than science, but they provide a reasonable way to associate the core business processes with suitable strategies to keep the business afloat and buoyant.

Crises are as inevitable as paying taxes and death. Whether you expend the energy to discover your risks or not and whether or not you successfully shape strategies to prevent, mitigate or control them, there will come a time when you and your CEO will come face-to-face with the iceberg. Facing the iceberg is managing risk.

Risk Management attempts to recognize and manage critical events caused by some risk. "What can go wrong?" "What existing situations have the potential to become crises?" and "What can be done to prevent or mitigate the impact?" are questions to ask during the Risk Assessment phase. "What contingencies can we use to respond?" and "What contingencies can we use to recover?" are questions that need answers throughout the time of crisis.

Where do you find the best candidates for prevention and mitigation? Former Martin Marietta CEO and chairman of American Red Cross, Norman Augustine, in his book Augustine's Laws gave us a "law" to help us think about prevention and

mitigation. His proposition is, “Tornadoes are caused by trailer parks.”¹ Each of us needs to survey our landscapes continuously for the “trailer parks” – the risks. Make a list of everything that could attract troubles to your enterprise. Get chummy with Murphy and his laws. Consider the possible consequences (impacts), and estimate the cost of prevention or mitigation. If the potential impact is high enough, the cause of the problem is in your enterprise’s control, and you can afford it – get it done! If you can’t do anything about it, unfortunately your organization is still not exempt from living with the consequences.

For CIOs, managing risk includes securing corporate systems, networks, and data; ensuring availability of systems and services; planning for disaster recovery and business continuity; complying with government regulations and license agreements; and protecting the organization against an increasing array of threats. For HR Directors, managing risk includes planning for emergency evacuation; recruiting temporary staff; protecting employee privacy and benefits; complying with government employee-related regulations; and ensuring means to communicate with all stakeholders. For all functions within the organization there are specialized Risk Management responsibilities.

On the other hand, there are a few *Universal Rules*² for managing risk:

1. Develop clear and robust management systems that are integrated with routine risk management processes. Increasingly, business crises are the result of the failure to have in place a system that enables management to spot and deal with risks expeditiously. During the first few minutes of the Three Mile Island nuclear power plant incident, there were over 100 alarms that went off, and there was no system for suppressing the unimportant signals so operators could concentrate just on the significant areas. A well-structured protocol is absolutely necessary for deciding when to define a situation as a crisis, when to take action and to work with others in solving the crisis. Once a crisis is recognized, it is all about seizing the initiative, and taking control of what has happened before it engulfs the entire organization.

2. Become a listening organization. Stop, look, listen. Watch for signs of trouble internally and externally. Create a list of “triggers” that can set off your radar before a risk becomes critical. Have contingency plans in place that can be whipped into action when one of these issues is triggered. Last year, the response to Katrina failed because authorities did not appreciate advance

¹ Norman R. Augustine, “Managing the Crisis You Tried to Prevent,” page 8, Harvard Business Review on Crisis Management, 2000. Harvard Business School Press.

² The general categories come from ideas expressed in Michael Regester & Judy Larkin, Risk Issues and Crisis Management: A Casebook of Best Practices, 3rd Edition 2005.

warnings (didn't listen) and were unable to quickly adapt response capabilities when the levees gave way. Literally, not much buoyancy there! Today, a much more complex and potentially devastating threat is looming, and instead of hours or days of warning, we have months or years of warning. Are we listening? Is that why only about 20% of all businesses are prepared for a pandemic?

3. Treat your stakeholders intelligently. Communicate with them. Let them know what is at risk and how each can play a role in protecting your most important assets: people, intellectual property and reputation. I might note here that in the wake of tsunamis, hurricanes, bird flu, war and terrorists, companies need to understand that these threats are real, even if these crises do not hit your company directly – because they could be collectively everybody's crisis! Your executive leadership is responsible for your organization, employees and stakeholders, and therefore, it is their obligation to deal with risks effectively.

4. Work as if everything you do and say is public. If you knew you were under the scrutiny of the media, how would that change what you do? It is important to build upon your enterprise's reputation and create an environment of trust – both valuable intangible assets, not tear these down during the heat of a crisis. What would President Bush have done differently if he knew the microphone was live during a lunch break at the G-8 conference in Russia in July of this year? It is best to avoid having to conduct damage control, especially when you are already in the midst of dealing with the huge iceberg that brought you here in the first place.

Summing it up. Some risks are potentially more dangerous or costly than others. Use a risk assessment to determine which risks have the highest priority and which ones you can effectively neutralize. Don't ignore problems. By heeding the warning signals and laying out protocol for managing risk, you will have an opportunity to protect your enterprise and its employees from the perils they face. Confront and resolve risks before they escalate into serious crises.

