

PREPARING YOUR BUSINESS FOR THE EVERYDAY DISASTERS

White Paper by Donna R. Childs

On May 30, the 2009 hurricane season begins and while forecasters expect an ordinary level of storm activity this year, we will still be watching televised images of storms in the Atlantic, most of which, thankfully, will not make landfall. Compelling images of damage wrought in the aftermath of major disasters, such as hurricanes and floods, are likely to capture our attention, but not likely to motivate effective measures to protect our businesses and families. How do we in the small business community explain this paradox? And what can we learn from it?

We are likely to discount these catastrophic events for being unlikely to happen to us. And most of the time, we are right: thankfully, few businesses will ever experience a Category 3, 4 or 5 hurricane, an earthquake that is 9 on the Richter scale or a terrorist attack such as what occurred on 9-11. And so we can justify not investing the time or effort in putting in place a business disaster plan for such a remote possibility. The relatively few businesses that are wrong, that actually do experience these disasters, will learn the hard way, the lessons of *ex ante* analysis. This focus on the catastrophic undermines effective preparedness and distorts perception of risk in a way that makes businesses more vulnerable even in the course of ordinary operations.

This concept runs completely counter to the conventional wisdom. Imagine a spectrum of risks. On the far left side, we have the “high frequency/low severity” risks or disasters. These are the everyday disasters, such as human errors, computer crashes, power outages such as blackouts and brownouts, and the like. These disasters occur all of the time, but they are not typically catastrophic. At the other end of the spectrum are the “high severity/low frequency” events such as major natural disasters: hurricanes, earthquakes and the like. Events such as fires, floods and environmental hazards fall somewhere in between.

SPECTRUM OF RISK

High frequency,
Low severity

High severity,
Low frequency

Examples:

- Human error
- Computer crash
- Power outage

Examples:

- Fire
- Flood
- Police action

Examples:

- Natural disasters
- Sabotage
- Terrorism

Categories:

- | | | |
|-----------------------|--------------------------|------------------------------|
| 1. Human errors | 3. Third-party failures | 5. Fires and other disasters |
| 2. Equipment failures | 4. Environmental hazards | 6. Terrorism and sabotage |

Source: Donna R. Childs. *Prepare for the Worst, Plan for the Best: Disaster Preparedness and Recovery for Small Business*. Second edition, Wiley, 2008.

We often focus on the catastrophic risks, those at the far right end of the spectrum. We assume that preparing for the worst-case scenario automatically subsumes preparation for all lesser risks. This approach generally holds true, but it should not form the basis of disaster planning. It hardly makes sense to initiate a full-blown disaster recovery plan every time the business experiences a minor deviation in operations. That is too expensive and cumbersome. And a focus on the catastrophic risk can induce paralysis, as staff reasonably fear that they cannot prepare for every contingency.

By contrast, the approach of preparing for the everyday disasters offers the following advantages:

- Immediate benefits
- Against more imminent threats
- At more affordable costs
- While building resilience to the more serious, but less likely, threats.

Consider, for example, a power outage. Power outages commonly occur on a stand-alone basis. They may appear as brownouts during the summer months during peak air conditioning usage or, more rarely, as an extreme event that left more than fifty million residents of North America without power for more than 24 hours. But power outages also commonly follow more serious disasters, such as hurricanes, earthquakes and terrorist attacks. By preparing the business for a power outage, the business would be ready for the more statistically likely threat, while building resilience for the less likely threat – the more severe natural disaster.

This lesson is illustrated every week in our financial capital, where everyday disasters are all too commonly the result of an aging infrastructure, such as the steam pipe eruption in mid-town Manhattan or the collapses of construction cranes that occurred last summer. These events follow a predictable pattern: the event occurs and emergency personnel immediately take to the television and radio news to reassure the public that there was no terrorism involved. But to the businesses that lost access to their premises as a result of the disruption, the result is similar to what happened to Lower Manhattan businesses in the aftermath of 9/11. Relatively few of these businesses sustained major property damage; the economic losses were typically the result of lost revenues or business interruption for which they were not prepared.

This framework is not limited just to Lower Manhattan post-9/11; it is universally applicable. Consider the experience of a daiquiri business in New Orleans that had successfully rebuilt from the losses inflicted by Hurricane Katrina. The owner of this small, but growing business was enjoying the winter, although he knew that the hurricane season would return again and he would again face the possibility of severe natural disasters. But he never had that opportunity, because his business burned to the ground in the off-season. He had not put data backups in place, because he was watching the hurricane calendar and thought that time was on his side. So the key message here is: prepare for the everyday disaster and this approach will address the more serious, and less likely, threats.

How should a business owner develop a framework for risk to guide staff in planning for contingencies? The framework of six disaster categories can be useful to guide business planning: human errors, equipment failures, third-party failures, environmental hazards, fires and other disasters and terrorism and sabotage. Human error, the most common form of disaster, is an error made by someone acting in good faith. The overall strategy to address this error is to ensure proper staff training and good management practices to reduce the frequency of this error. For example, if your department always manages in a crisis mode, the resulting stress may make your employees more prone to errors. If you can revise your management practices to reduce the stress levels in the workplace, you will likely see a commensurate reduction in human errors. Once you put in place a strategy to reduce the frequency of human error, you need to have a strategy to mitigate its cost when it does occur, such with on-demand user-generated data backups, for example, and clear recovery procedures.

Equipment failures are partial or total malfunctions of machinery that is necessary to run the business. Here the strategy is to reduce the frequency of occurrence, by making good vendor selections and following proper equipment

maintenance procedures, and building in redundancy for when those failures will occur. So you should have extra equipment in inventory. Third-party failures are the failures of service providers needed to deliver the products and services of the business. This would include much of what we see in the current credit market collapse and counterparties lack faith in one another and deteriorating conditions raise the risk of default. Here the basis strategy is to invest in due diligence to make wise choices for third party vendors to which to entrust your critical services, negotiate appropriate service guarantees and support and build in redundancy to cope with failure when it will occur.

UNIQUE RISKS – UNIQUE PREPARATION



While frequency of risk decreases, other risks, such as data security, may increase

Features	Unintentional errors	Malfunctions or complete failures of machinery	Failures of service providers	Conditions that displace you from your worksite	Fires and natural hazards	Intentional systematic campaign to cause harm
Risk category	Human errors	Equipment failures	Third-party failures	Environmental hazards	Fires and other disasters	Terrorism and sabotage
Unique response	Investigates issues related to training – these can erode productivity, sign-off for backups	Examine set-up and maintenance programs, predict failures	Invest in due diligence, service guarantees and redundancy	Plan for human safety and temporary remote operations	Plan for more severe threats to human safety and longer periods of remote operations	Be aware of the psychological and emotional needs of employees

Source: Donna R. Childs. *Prepare for the Worst, Plan for the Best: Disaster Preparedness and Recovery for Small Business*. Second edition, Wiley, 2008.

Environmental hazards are conditions that displace staff from the worksite. These need not be Love Canal type events; they could be as trivial as a water pipe bursting flooding the office and then improper cleaning of the original damage resulting in mold spores in the office, which extend the period of displacement. Here the overall strategy is to plan for human safety and temporary remote operations. This concept is extended for fire and natural hazards, which pose more severe threats to human safety and longer periods of remote operations, as well as terrorism and sabotage. With respect to the latter category, the business cannot be fully prepared for terrorism and sabotage; however, everything that is done to prepare for the lesser risks will be critical.

Now that the framework has been presented, the next step is to identify the key assets of the business. This may sound simplistic, but it is not necessarily obvious. Consider the example of a small software development company that had insured its property against the risk of disaster. When it subsequently experienced a total loss of its physical assets due to a fire, it was fully reimbursed for the replacement costs of its office furnishings. But this is not what drives

the valuation of a start-up software company; its critical asset is its intellectual property, embedded in hundreds of thousands of lines of software code its programmers had written. The company had failed to make backup copies of the software it had developed and subsequently went out of business. If it had a severe budget constraint, as start-ups often do, it would have better served to forfeit insurance on the physical assets and invest the premiums saved in off-site secure data backup.

Another example might be a restaurant chain; Ruth Chris's Steak House is a well-known example of a restaurant that worked through severe hurricanes. For the restaurant, customer access to the premises is critical, so it would likely make sense to invest in business interruption insurance to replace revenues lost when the business cannot open for customers. Another critical consideration is the costs of food spoilage that, for a restaurant in a large city, could run \$50,000 for a 24-hour outage. Commercial insurance policies don't ordinarily cover this risk, which is why the restaurant should elect an endorsement (an insurance term for "add-on") for the interruption of electrical supply so that this loss would be indemnified. Restaurants, grocers and other food service businesses often run on such narrow profit margins that the loss due to spoilage for a 24-hour power outage could impair their ability to make payroll the following week.

You can appreciate that there is more than one benefit to this approach. In addition to determining how best to protect the business in the event of a disaster, this exercise motivates some useful insights as to how to better manage the business in the course of normal operations. Consider the recent experience of the City of San Francisco when a disgruntled systems administrator refused to relinquish key passwords to computer systems controlling, among other functions, employee payroll. The Mayor of San Francisco had to visit the systems administrator in jail to meet his demands to turn over the password. In the framework presented here, this qualifies as "sabotage", an extreme event. But what if that systems administrator had suffered a medical emergency or a car accident, two statistically more likely events? The result would likely have been the same: the operations of the City government would have ground to a halt because of this critical dependence on a single systems administrator. A little due diligence to understand the key processes, assets and functions of the City's operations might have revealed this vulnerability such that it could have been remedied in a timely manner – before the systems administrator decided to wreak havoc with San Francisco.

This common-sense approach – view the framework for everyday disasters, identify the key assets and processes of the business and manage the risks accordingly – yields immediate benefits that your business can realize, *even if disaster never strikes your business*.



Donna R. Childs is the author of *Prepare for the Worst, Plan for the Best: Disaster Preparedness and Recovery for Small Businesses* (Second edition, John Wiley & Sons Inc., 2008). She was formerly based in Zurich, Switzerland where she was a senior executive of the world's largest property-casualty and life-health reinsurance company. Her responsibilities included advising "C" level executives of global corporations in respect of their risk management and business continuity strategies. This experience proved critical when she returned to the U.S. to start her own business, which was located in the immediate vicinity of the World Trade Center on 9-11-01. Because of its exceptional level of preparedness, Donna's business is profiled in the "Ready for Business" campaign of the Department of Homeland Security.