CRISIS AND LEVIATHAN

1

Yes, You Should Sweat the Small Stuff!

Disasters occur more frequently than we realize. Research consistently shows that for small businesses, the effects of a disaster can be devastating:

- More than one in four businesses will experience a significant crisis in any year.[1]
- Of those businesses that experience a disaster and have no emergency plan, 43% never reopen.[2]
- Of those that reopen, only 29% are operating two years later.[3]

The losses that these figures represent do not appear to have motivated preparedness efforts by small businesses: A recent survey of 2,500 small business owners found that 71% did not have a disaster preparedness plan in place. Nearly two-thirds of them stated that they do not need one. 63% expressed confidence that they would resume business within 72 hours if they were affected by a natural disaster, even though historical experience shows that this is absolutely not the case.[4]

Disasters are, for the most part, manageable. We cannot prevent disasters from occurring, but we can equip small business owners with the knowledge that they will need to mitigate their risks and to recover quickly when disasters do strike. That is the goal of this book.

As small business owners, our resources are limited and we must work our assets smarter, not harder, than the assets of larger companies. We must spend our insurance premium dollars wisely and make cost-effective decisions

on establishing backup information technology (IT) support. In the first edition of this book,[5] Stefan Dietrich and I provided our readers the tools to put in place an appropriate contingency and disaster recovery plan. This second edition has been updated with all-new material, drawing on the experiences small business owners around the world have shared with me since the first edition was published. This second edition also features new material about disaster recovery programs, as we were still working through the process with the Federal Emergency Management Agency (FEMA) and other relief agencies when our first edition went to press. Now that time has passed, I can share with you more information about how that recovery process works. If I were ever, heaven forbid, to experience another major disaster, there are certain "assistance" programs that I would avoid. Now that I have fully completed the recovery process, I can share these insights with you.

Before continuing, let's be clear about what we mean by "disaster." A disaster can be defined as an event that disrupts business operations at a given site and results in a temporary or permanent dislocation of the business. A factory fire is, by this definition, a disaster. A product liability crisis, by the same definition, is not. Consider Johnson & Johnson's 1982 experience of tampering with its Tylenol® product. That is a business crisis, one that requires careful management of communications with stakeholders and possibly changes to business (or in this case, packaging) processes. The Tylenol® crisis, while undoubtedly painful for the company, did not disrupt business operations or cause employees to lose access to Johnson & Johnson facilities. Work at Johnson & Johnson continued on-site, even as the company's executives worked to communicate with their customers, the investment community, the distributors of their product, and other stakeholders. I cannot advise you on situations such as the Tylenol® crisis; this is not my expertise. As such, crisis management is beyond the scope of this book and I would refer you to other sources.[6]

Few small business owners have the reach to find themselves in a crisis comparable to that of Johnson & Johnson. However, many of us will, unfortunately, experience natural disasters such as fires, floods, and disruptions in power supply during the course of building our businesses. Carefully crafting an insurance program and ensuring adequate IT capacity can mitigate the consequences of such disasters. Many of the techniques and suggestions in this book are applicable to the nonprofit sector as well. Nonprofit organizations, like small businesses, pursue their missions with limited resources and may benefit from putting in place a disaster preparedness plan.

Of course, each small business (or nonprofit organization) faces unique circumstances and constraints and no one can reasonably anticipate the needs of each and every single reader. It is best to consult experts, such as commercial insurance brokers, where appropriate, and expect that the information in this book will enable you to be a more knowledgeable consumer of such services and to use such services in a cost-effective manner.

I hope that your business never experiences a disaster. Unfortunately, we cannot prevent such tragedies from occurring—and they do occur from

time to time. However, I hope to assist you in preparing your small business when disasters happen. I also believe that you will find that contingency and disaster recovery planning improves the efficiencies of your business processes and therefore, the planning process will immediately benefit your business—*irrespective of whether your business ever experiences a disaster*. Now that I have outlined what we hope to accomplish with this book, let us begin by debunking a common myth.

It is commonly believed that preparing for the worst-case scenario automatically subsumes preparation for all lesser risks. This assumption should not form the basis of your contingency planning. Do you really want to initiate a full-blown disaster recovery every time you experience a minor deviation in business operations? That is not a very efficient way to run your business. There are also other reasons why this myth must be exploded:

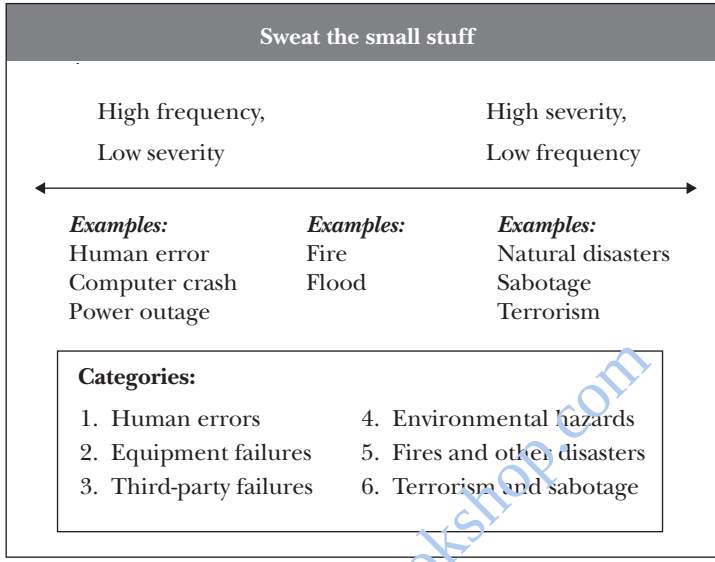
- **It Induces Planning Paralysis.** If your entire preparedness effort is focused on the catastrophic event, you are likely to do nothing at all. Why? Because you can (quite reasonably) discount the likelihood of the catastrophic event occurring, leaving your business vulnerable to less severe disasters. Imagine sealing your office with duct tape for fear of a dirty bomb and then losing all of your business-critical data because of a power outage. It is ridiculous, isn't it? But that is how disaster preparedness is sold to the public.
- **It Distorts Assessments of Risks.** Have you seen people wearing t-shirts with glib slogans about how everything is going to seed anyway, so you may as well surrender to the flow? By looking at catastrophic scenarios, you are tempted to say to yourself, "Well since I cannot prepare for everything, I guess I will prepare for nothing." This type of feigned helplessness is poison for your business.
- **It Fails to Provide for the Benefits of Responsible Behavior.** Building disaster-resilience into your small business will *provide immediate benefits to your business even* if disaster never strikes. Later, in the section titled "Preparation Pays" I will show you how.

I would like to propose another perspective on risk: the one used by reinsurers and risk management professionals. In this chapter, I will present the model of building increasing organizational resilience and (I hope!) de-bunk the myth that small businesses should prepare for the worst-case scenarios.

SPECTRUM OF RISK

In the reinsurance industry, we typically evaluate risk across the spectrum from the high-frequency/low-severity events (the "everyday" disasters), such as human errors and computer crashes, to the high-severity/low-frequency events (the "catastrophic" disasters), such as earthquakes and hurricanes.

Exhibit 1.1 Risk Spectrum



Often, small business owners forego contingency planning for disasters, believing disasters to be catastrophic in scope and beyond their control. In fact, the "disasters" your business are most likely to experience are of the mundane human error variety. Although often trivial, human errors may have severe consequences. Consider that the root cause of the 1986 Space Shuttle *Challenger* disaster was human error. More recently, the runways at Los Angeles Airport were closed for several hours due to human error.

There are procedures that you can put in place to mitigate your business losses from such disasters. Those procedures, in turn, will help you build more resilient and robust business processes, better equipped to recover from the larger-scale disasters. Let's examine six categories of disaster in more detail (see Exhibit 1.1).

1. **Human Errors.** Human errors are triggered by actions unintentionally undertaken by managers and employees acting in good faith; actions that are subsequently shown to be mistakes. The most common causes of human errors are inadequate computer-user training, fatigue, and carelessness. These errors can reduce productivity and increase the costs to your small business.

   Real-world example: A new employee at a small business client support group wanted to add new phone numbers to the contact information in the company's call tracking system. He thought that instead of entering

the telephone numbers manually, he could save time by writing a script that would automatically replace the appropriate numbers. Upon running the script, all phone numbers in the system were replaced with the first phone number in his script. It took hours to retrieve the backup tapes and to rebuild the database. All the updates made to the computer system that day had to be manually corrected—the original task the new employee had sought to avoid became the least time-consuming part of the recovery process.

2. **Equipment Failures.** These are malfunctions or complete failures of any type of office machinery used to store or to process information. Office equipment commonly includes fax machines, personal computers, phone systems, and network components. Equipment is prone to breakage and failure, and so you should anticipate that your business will, at some time, experience equipment failure.

   Real-world example: After five years (!) of service, the main disk of an old file server would no longer spin after the machine had been routinely rebooted. Subsequent investigation revealed that none of the remaining computers could read data from that main disk. After comparing the costs of hiring a data recovery service to reestablish the data and the hours required to restore the data from the backup system, it was determined that only about 20% of the most critical business data would be recovered, leading to great frustration among the employees who had lost files.

3. **Third-Party Failures.** These are failures of third parties to deliver services that you need to operate your information storing and processing equipment. Included here are electrical power failures, loss of phone service, or failures of Internet or market data providers. This category also includes financial disasters (e.g., the default of your largest customer).

   Real-world example: A telecommunication provider defaults on its debt and seeks bankruptcy protection. Your business telephone system malfunctions. Your service provider informs you that they are using the services of a repair company that also had to temporarily suspend its services because its main creditor was the telecommunications company now in default. You are assured that everything is being done to fix your phone connection as soon as possible, but with other "big" clients on their priority list, you, a small business owner, have to wait a couple of days. When you go home in the evening, your answering machine is full of messages with urgent calls from your clients.

4. **Environmental Hazards.** These are all conditions that do not permit you to enter your regular business offices while your IT infrastructure stays operational. These conditions could include smoke from a nearby fire, hazardous substances discovered in your building, irritants

like fresh paints, pollutants in your building, or contamination of your office with either radioactive, biological, or chemical substances. These hazards prevent you from entering your worksite.

Real-world example: Asbestos is discovered during construction work in your neighbor's offices. You share the same air conditioning unit and you have to leave your offices. You are not allowed to take any computer equipment with you as the fans have collected asbestos with the dust and require cleaning that will take days to complete.

5. **Fires and Other Disasters.** Here we consider all events that are destructive to your office and hence, to your IT infrastructure. Although fire poses the most common threat, other disasters include natural events, like earthquakes, floods, storms, and man-made disasters, like gas leaks and subsequent explosions. All of these can be very destructive and would render your office unusable or simply prevent your key employees from coming to work.

   Real-world example: A water pipe in the ceiling broke. Water sprayed throughout the office. Eventually, it seeped into some IT equipment and short-circuited the power supply. Fortunately, the water was quickly shut off, the equipment dried, and some parts, including the power supply, replaced. Everything seemed to be fine. Two weeks later, severe mold developed. A hazardous condition existed and the office could no longer be used. The IT equipment was relocated to a temporary office location, but the equipment became unreliable. Water corrosion inside the PC damaged plugs and prevented the central processing unit (CPU) fan from running at full speed. Insufficient cooling of the CPU caused system crashes. This is a good example of how a single event can cause a series of related disasters, in this case, from a water leak to equipment failure.

6. **Terrorism & Sabotage.** A terrorist attack is an intentional, systematic, planned, and organized effort with the goal to cause maximum damage with resulting publicity. Sabotage is also motivated by calculated intent, but rarely attracts the same level of public attention. Unlike the other disaster types, acts of terrorism and sabotage can be the most threatening because they are based on malicious intent; and if the perpetrators have access to sensitive information about your business, very concentrated damage can be done with relatively little effort. For terrorists, all means are considered just to reach the goal. Hence, the spectrum of attacks is unusually large, from hostage situations to large bomb explosions, and, as we saw on September 11, suicide missions using planes as weapons of mass destruction. Saboteurs, however, like the secrecy of underground activities and work with sophisticated tools. They can attack you from the outside (e.g., attacks by computer hackers), or attempt to infiltrate your organization with computer

viruses. You can also be struck from the inside when, for example, a disgruntled system administrator sabotages your backup system.

Real-world example: These are rare cases, and unfortunately, practically impossible to be fully protected from. Terrorist acts are usually public and can result in the complete destruction of IT assets. Cases of sabotage seldom reach the public's attention, and it cannot always be determined if the damage was the result of a highly sophisticated act of sabotage or simply a common equipment failure. Since it is not a good idea to make suggestions to those with bad intentions, let's refer to a real-world example from 20 years ago. A company with approximately 40 employees had a so-called minicomputer and a green bar paper printer, both of which were located in an air-conditioned room. The company depended on this one computer system, as the cost to back it up with a second system was simply prohibitive. However, the operating system was very stable, so typically this was a very reliable setup. An employee, possibly by accident, reduced the level of humidity in the air quality control unit resulting in the buildup of high electrostatic voltage in the printer paper. The voltage was discharged through the connection of the computer with the printer, thereby destroying the whole computer.

Each category of disaster requires a unique form of preparation and emergency response. In developing your business contingency plan to protect against these disasters, you should consider that as you cross the spectrum from Human Error toward Terrorism and Sabotage, the frequency of the event decreases but the severity of the resulting damage increases. Human error is by far the most common cause of business disasters on a day-to-day basis. In most cases, it is relatively simple to protect against this risk and it is possible to recover from such errors with minimal impact to your company's business. However, an act of terrorism and sabotage would be a rare event for most businesses, but should such an event occur, it would cause significant damage that could critically affect your company's future. Thus, it is important for you to weigh the likelihood of occurrence with the risks associated with each type of disaster in order to create the type of disaster contingency plan that best meets your needs.

EVERYDAY DISASTERS CAN HAVE SERIOUS CONSEQUENCES

How many times have you watched in horror as the evening television news shows images of frustrated small business owners dealing with computer-related disasters? I cannot think of one example from my own experience. But if there is a car accident on the highway, it will likely lead the evening news. Television news depends upon highly visual, graphic images of disasters and

as such, tends to distort our perception of risks. Let's consider a series of true case studies involving computer-related disasters that small businesses deal with every day.

Online antiques dealer disabled by a virus

FromGlobaltoYou.com is an online antiques business based in Utah that was struck by the Klez e-mail worm. Notwithstanding the fact that the company had installed anti-viral software, the worm flooded employees' e-mail in-boxes and locked up its ten desktop computers, shutting the business down for two days. As a consequence of this disruption, FromGlobaltoYou.com permanently lost about 30 customers who were disappointed with the poor service and e-mail spam caused by the virus. In addition, the Company lost a significant amount of revenue from eBay auctions because it couldn't complete sales before getting back online. As a result, the Company's expansion plans were delayed for nearly two years. The co-owner of the business, Dianne Bingham, said, "small- and medium-sized businesses never think it can happen to them, but it can and the results can be devastating."

Now we don't see e-mail worms on the television news, but they can do as much or more economic damage than fires! Let's consider another, related, example.

Newspaper disrupted by server virus

Providence Business News serves readers who work for growing businesses in Rhode Island and nearby Massachusetts. The newspaper had carefully backed up its key data and had, on occasion, experienced minor viruses on local workstations. However, around Thanksgiving 2004, a virus infected the e-mail server and disabled the entire system. The backups were infected with the same virus that had disabled the main server. Staff coped by using G-mail and Yahoo e-mail for six weeks until the newspaper was fully back online. According to *Providence Business News* Publisher Roger Bergenheim, "You don't realize how much you depend on e-mail; at this point it is more important to business than the telephone."

Imagine that you have your employees running from your office to the local copy center so that they can rent computers by the hour from which to send e-mails across Web services. That is not the type of disaster the media will cover, but it is certainly disruptive and costly. The following is another example.

Online pet retailer loses a week repairing damage done by a virus

Kitty's WonderBox® was founded in 1991. The company grew out of a product concept for an easy, convenient, and disposable cat litter box. In 2004, the company's systems were infected with a virus, which required that the management team purge and rebuild many of their files. The company had backups, but getting everything back online took a week of their time. Said company CEO Riza Chase-Gilpin, "I can certainly attest to having a good support IT person or company in place when disaster hits!"

Let's move from viruses to equipment failures.

Busy restaurant experiences disk crash

Komegashi is a chain of Japanese restaurants that does an active business serving customers dining in and taking out meals. Each restaurant organizes customer data electronically by telephone number for ease in retrieving information for takeout orders (such as the customers' addresses, directions to their homes, etc.). During one busy dinner shift, the hard disk of one restaurant's computer overheated, causing the disk to crash. The customer data were destroyed. General Manager Carol Hu said, "the computers are powered and in constant use, and our database is enormous as customers who relocate often remain in our system. It is an enormous amount of work to maintain such a database reliably."

Here is another example:

Seminar interrupted by a defective video card

Theweleit Consulting is an engineering firm based in Cologne, Germany, focusing on energy-efficient solutions. The consultants often use laptop computers to work on-site with clients. Minutes before an important presentation, the laptop's video card failed.

Although a replacement laptop was quickly found, transferring the presentation files was a challenge. Sending the laptop in for repair could have meant potentially destroying the data, which had not been backed up. Finding an IT expert to repair the laptop while preserving the data without any screen required a great deal of effort and several days of work.

Then, there are the old-fashioned power outages.

Power interruption disrupts physician's office

Dr. Schmidt maintains a medical practice in Kassel, Germany. An overnight interruption in the electrical supply caused the two PCs running physician practice management software to reboot. The following morning, the staff noted that there had been a power interruption that caused the system to reboot, but as they detected no other anomalies, they continued to enter new patient records into the system. Several days later, the staff noted that the database had been corrupted by the unclean system shutdown caused by the power failure. It took several days of work for the staff to manually compare the patient's paper records with the data in the computers, and to merge the old with the new records entered since the power failure.

Let's not forget the basic disaster, human error.

Australian firm loses valuable time and data in upgrading its server

IRC is an independent consultancy in Australia providing risk management and engineering services to the energy industry. The company used two servers, one as a mail server and the other as a file server. Although backup measures were in place, when the company sought to upgrade to an advanced server over one Christmas break, they learned that the installation parameters were not exactly the same on the new system as on the existing system, causing staff to lose four days of valuable time and a small amount of unique information not available on the backup. The system was restored 100% when IRC performed a complete rebuild several months later. "Although from a technical standpoint it sounds like a minor problem, the loss of e-mail data and communications for that period had the potential to delay projects by several days. Many of our projects are short duration with tight deadlines—a four-day delay can have major implications for our clients," said Colin Wright, a cofounder of IRC.

Or, how about a one-two punch?

Filmmaker's studio loses data

Gypsy Heart Productions is the brainchild of Jocelyn Ajami, an artist and independent filmmaker whose recent work debuted at the Museum of Fine Arts in Boston. Jocelyn maintains an extensive digital library of her work and sustained a "one-two" punch when she lost data due to a power outage, and then a subsequent data loss when a new virus, unidentified by the antiviral software she was using, infected her system. "Everyone I know has experienced this," she said. "It is just so frustrating to have this downtime."

Unlike large corporations, small businesses have limited resources. We simply cannot throw more people at the problem or keep enormous stocks of reserve equipment for when the video card or the disk fails. It is the smaller, "under the radar screen" disasters that can be ruinous.

Let's close with one more example before moving on to the next section. Do you recall that emergency officials in Canada had to evacuate a good part of Newfoundland when Hurricane Juan moved up the Atlantic Coast? If you are from Canada, then you likely remember this one. If you are from elsewhere, think of the Asian tsunami or Hurricane Katrina or your local major natural disaster. Now, what if I told you that the economic losses borne by local small businesses were far greater due to over-fishing off the coast of Newfoundland than the economic losses caused by the hurricane? The disruption of the fishing industry had a "domino" effect on the local economy. Imagine that your small business serves a clientele of local fisherman or that your restaurant purchases from the local fishmongers. The consequences of Hurricane Juan were not as devastating. Yet, that is not how we think of risk.

The following are the key takeaways from this section:

- You are, by definition, more likely to experience a high-frequency disaster than a high-severity one.
- High frequency, or "everyday" disasters, can be painful and costly.

TACKLING RISKS ONE STEP AT A TIME

For these reasons, it is best to begin by preparing for the "everyday" disasters to incrementally build resilience to more serious forms of disaster. Let's consider the example of a power outage. Power outages can occur on a standalone basis. In the summer of 2006, thousands of small businesses in Queens, New York, were without electricity for as long as nine days. Some grocers and restaurants were financially ruined as a result of the outage. Perhaps an example that is better known is the power outage during the summer of 2004 that left 50 million residents of the United States and Canada in the dark. Less well-known are the episodic interruptions of power in the affected areas during the weeks following the major blackout, after power was officially restored. So a power outage is a disaster in its own right.

It is also a common occurrence in the aftermath of more serious forms of disaster, such as hurricanes, earthquakes, and terrorist attacks. If you develop a plan for how your business would function with a disruption in the supply of electricity, you are automatically better prepared for coping with the more serious forms of disaster.

For another illustration of this concept, let's return to our case study of the filmmaker who lost her digital files due to a power outage and later a virus. Those files are gone forever and they are her creative work product.

What if she had backed up her digital files off-site? Then she would not only have been better prepared for the power outage and the virus, but she would also have been better prepared for a possible fire.

For the record, my disaster preparedness plan never contemplated anything on the scale and scope of what I experienced on 9/11. When I began thinking about risks to my business, I had two "worst-case scenarios" in mind: a fire in the nearby Wall Street subway station or an event similar to the scaffolding accident that had occurred near Times Square that caused small businesses within a radius of many city blocks to lose access to their premises. Yet the disaster preparedness plan I put in place was sufficient to see me through something far worse.

In Chapter 2, we will consider incrementally building resilience to disaster, starting with addressing the risks of human error and moving on to more serious threats. But before we dive into the specifics of planning, I want to conclude this chapter on a positive note.

PREPARATION PAYS

Many people mistakenly believe that preparing for disaster is time-consuming and costly. This is another myth that I hope to debunk by the end of this book! You should not think that if you invest time and effort in preparing your business for disaster, and the disaster does not occur, that it was all for naught. Investing in disaster preparedness yields an immediate return, *even if disaster never strikes*:

- **You Can Decrease Your Expenses.** I negotiated double-digit percentage decreases in my commercial insurance premiums by sharing a robust disaster preparedness plan with my insurance company. I demonstrated that I was a better risk than my peers and argued that my improved risk profile should be reflected in a lower premium.
- **You Can Increase Your Opportunities to Grow Revenues.** As part of their own contingency planning, large corporations are increasingly looking at the resilience of their supply chains. As part of their due diligence, they are evaluating how prospective vendors would meet their deliverables in the event of a disaster or severe disruption. To the extent that you can build confidence that you have a methodical disaster preparedness plan, you are more competitive to win the business.
- **You Can Increase Your Operational Efficiency.** The process of developing a thoughtful preparedness plan involves doing process engineering on how your business works. This process will inevitably yield insights into how you can run the business more efficiently. I will highlight specific examples later in this book.

Let's be pragmatic: From time to time, bad things will happen and it is best to prepare for them as well as we can. Then we can sleep soundly at night knowing that we have acted responsibly to ensure the safety of our families and our employees.

NOTES

1. This was the finding of a January 2005 survey conducted by *Continuity Insights* magazine and KPMG Risk Advisory Services.
2. The Hartford's *Guide to Emergency Preparedness Planning*, The Hartford Financial Services Group, published in 2002.
3. *Ibid.*
4. See www.officedepot.com. This survey was conducted in February 2007 for Office Depot.
5. Donna R. Childs and Stefan Dietrich, *Contingency Planning and Disaster Recovery: A Small Business Guide*, John Wiley & Sons, 2002.
6. During the course of my business career, I participated in excellent crisis management programs offered by the Corporate Response Group in Washington, DC, which I highly recommend.