CHAPTER 1

Preparation

The first step in preparing a disaster contingency plan is a rigorous assessment of your business. In this chapter we are going to guide you through a plan of preparation for your critical IT assets and for a program of insurance. We want to share with you what we have learned about the need to put in place redundant technology and financial assets so you can recover more quickly when disaster strikes. We preface this guide with some questions for you to keep in mind as you work through this section of the book. The questions that we hope to provoke, and the answers that only you and your employees can provide, will help you to identify areas on which to focus in developing your contingency plan.

You must identify the critical business assets that you wish to protect. Now is the perfect time to assess past events that have affected your business (Have you had prior experience with natural disasters? Is your business located in a flood zone?) and your business's current status. Consider how you would react to the categories of disasters we have identified and take into consideration how your clients and suppliers would be affected should your business experience a disaster. For example, if your business operations were temporarily disrupted, would your clients seek alternate sources of the products and services you supply to them? Could you mitigate this risk by diversifying your production and operations sites? Would your suppliers have difficulty sending shipments to an alternate business location that you might use on a temporary basis?

Given the existing resources of your small business, define the scope of the endeavor that you think is reasonable. Define some intermediate goals and estimate the costs of developing your contingency plans rela-

tive to the potential benefits. You will have to make some assumptions, and you will have to identify some risk factors for your business. For example, contingency plans have most often included the provision that only one building will be affected in a disastrous event destroying the site, but the attacks on the World Trade Center invalidate this assumption in cities with major structures that could be attacked from the air.

You also may have to consider a wider range of disaster-affected areas as you begin to develop your contingency plan. A former colleague works in a small business in Lower Manhattan that backed up its data nightly and placed those backup tapes securely in a bank safe deposit box. Unfortunately, that particular bank branch was located in the shopping concourse of the World Trade Center. I (Donna) used to bring backup CDs home with me when my contingency plans contemplated worst-case disaster scenarios such as a fire destroying my office building. I had not contemplated a scenario that would simultaneously affect both my home and my place of work. I have since revised my contingency plan for recovering electronic data.

Developing your contingency plan should not become a large bureaucratic effort. Indeed, to be effective, your small business's contingency plans should be a model of clarity, understood by every member of the company. It begins with key management leaders and includes all of the employees, because in a disaster situation every person who is knowledgeable and prepared can make a critical difference to a successful outcome. Employee training is key, because each person must understand the importance and necessity of contingency planning and response to a disaster and know what his or her role will be. In a real emergency you cannot afford to delay your response because roles had not been clearly defined. Indeed, we would like to suggest to you that in order to build employee consensus about the need for contingency planning, you educate your employees and encourage them to develop their own personal and family contingency plans. Such an effort will likely yield extraordinary dividends—small businesses are often wonderful places to work in part because we are like families, not large, impersonal bureaucracies. The sincere care and concern you show for your employees will result in higher productivity.

To illustrate our point, we would like to share with you three real and painful stories of families that suffered in disasters. These are examples of suffering that could have been alleviated had the families done some personal contingency or disaster planning. The first concerns a friend

who suffered a head injury from the force of falling debris in a burning building. His relatives almost certainly saw the disaster reported on the local television news. Imagine the mental torture they suffered as they worried about what had happened to him. If he had maintained an "In case of emergency . . ." card in his wallet, medical staff who treated him could have contacted his relatives and informed them of his status. Until he was able to communicate himself (he was heavily sedated following major surgery), his relatives were left to frantically call his apartment in the hope that he would answer or return the messages that they had left on his answering machine. We both have nurses in our families, and each of us has a laminated card in our wallets advising whom to contact on our behalf in the event of an emergency. We provide secondary contacts in the event our first contact cannot be reached. We also recommend that you verify this information annually because people do move, change employers, and so forth, and outdated information is of little use.

Let us give you a second example. I (Donna) was told the following story by a neighbor. We have a neighbor who worked in the World Trade Center and has not been seen since September 11. She is presumed to be dead. Her father came to New York City to inquire if anyone had seen her and showed photographs of her to the other tenants of the building. This lady had day-care arrangements for her child, but no one, including the child's grandfather, knew what they were. Presumably, the day-care provider had been given an emergency contact person, but imagine the anxiety that the child's grandfather suffered that might have been mitigated if he had been made aware of the child-care arrangements and knew how to directly contact the day-care provider.

Finally, I want to share with you a personal example that had a happier ending. My (Donna's) mother suffered a traumatic head injury that required extensive medical intervention. My parents, as part of their contingency planning, had prepared advance health-care directives and durable powers of attorney in the event that one or both of them should become incapacitated. I was able to sign consent forms authorizing the forms of treatment that were consistent with her wishes. (I'm happy to report that she is alive and well.)

Most people generally don't give such thought to these matters. We are not by nature ghoulish, but we each have nurses in our families and my (Donna's) grandfather was a firefighter, so we probably have a greater awareness of the incidence of disasters. We don't intend that our loved ones should suffer needless worry about us and you shouldn't either, and

neither should your employees. Encourage your employees to bring the methodology of contingency planning and disaster recovery home with them. Make them aware of the first aid classes that are offered by the Red Cross. Ask them if they can remember when they last replaced the batteries in their smoke alarms at home. It is hard to concentrate on the business task at hand if you or your employees are worried about the safety of your families. If your son was missing following a disaster, how productive would you have been at work during the period that he was unable to call you and the medical staff treating him had no family contact information? Make careful planning a way of life and of business for everyone in your extended small business family.

You will also discover that you should do some general process engineering on how your company works. If your business has clear lines of responsibility, defined processes that are established and followed, and documents that are properly filed, you will likely be successful in establishing a good disaster recovery scheme. If your normal business day is characterized by managing the crisis du jour in an atmosphere of confusion, you will likely have difficulty implementing a disaster recovery plan.

Many companies that we visited were actually not ready to implement disaster recovery solutions. Many of them had gone through so many computer and system upgrades, using many different "bundled" applications, that they were faced with not only a wide collection of similarly named documents in various locations, but they also had documents that could not be assigned to any former activity because it was no longer possible to read them without going through a major deciphering effort. This is much more an issue for small businesses, because large businesses usually have standardized roll-out IT platforms and consolidated user data storage.

Now you understand why any contingency planning effort must be conducted in concert with a major review of your business, not only to identify the critical assets that you need to protect, but also to identify and organize all related items. As you can imagine, although it will be time-consuming at first, your small business will benefit as a result.

Once you have reviewed your business operations, you will be ready to order your priorities and select the areas on which to focus. Some of these areas you may consider because they are located in offices that appear to be at high risk. You may consider other offices as candidates for a contingency provision with a remote backup site. An alternate

business site is needed if your original site is out of service or inaccessible. An excellent solution for small businesses with multiple sites of operations is to share disaster contingency space distributed over all of your offices or other facilities. So if one business location goes down, the other locations would provide space and IT services for some key employees. You could also consider integrating a telecommuting setup in your temporary disaster recovery provisions whereby key employees would work from home using services provided from an off-site IT setup.

Once you have developed a thorough plan, you must be prepared to revisit it regularly and revise it, if necessary. Take the opportunity to schedule a disaster shutdown of your company's operations, for example, on the weekend following a regularly scheduled fire drill. Once your backup location is ready, you should regularly update and train your key staff on disaster mode operation. As your small business grows, your needs will change and you will need to adapt your disaster contingency plan accordingly. We also advise you to prepare an inventory of your property, plant, and equipment.

For IT assets you need to keep a record of:

Hardware assets: manufacturer, model name and number, quantity, serial numbers, service tags/configuration code, maintenance dates, support phone, location, and replacement cost.

Software assets: manufacturer, title, version, quantity, serial number/license key, support phone, location, and replacement cost.

IT staff/human capital: employee's name, position, telephone (work, home, mobile), and responsibility during disaster.

System data assets: system name, operating system, location, if backup unit available and where, backup frequency, and person responsible.

User data: system name, operating system, location, if backup unit available, location, backup frequency, and person responsible.

Third party: service name, provider name, and phone (support desk, emergency number).

Printers, network, and other peripherals: manufacturer, model name and number, serial number, maintenance dates, phone (support desk, emergency number), and replacement cost.

This information will be important in your recovery efforts as you need to know which equipment (and which personnel) can be redeployed and which assets your insurance policy may replace. Now that we

have completed our "preparation" overview, we are ready to "drill down" to specific areas on which to focus in developing your contingency plan. In this chapter, we discuss topics such as proper handling of office mail, developing an IT infrastructure, and putting together an insurance program. Before we delve into the specifics, however, we would like to conclude this section with two thoughts.

First, notice that this chapter (Preparation) is longer than the following two chapters ("Response" and "Recovery"). We didn't plan it that way, but we noticed that was the result when we completed our manuscript. That *should* be the result: planning is the most important activity you will undertake. Risk management and disaster recovery specialists have an expression: "To fail to plan is to plan to fail." The time and effort you invest in preparation will expedite your recovery from disaster.

The second point we would like to emphasize is that because successful contingency planning is closely connected with a thorough understanding of your business operations, contingency planning almost always yields benefits to your business—even if disaster never strikes. I (Donna) know a small financial services company that began to consider how it would treat mail delivery following the anthrax scare in the fall of 2001. As the company began to review its existing procedures for handling mail, it discovered something shocking: it was spending $9,000 annually to send interoffice documents by overnight express delivery, when an electronic document delivery system would have done the same work at negligible cost. Now, $9,000 is a lot of money to a small business, and we are certain that any small business owner can think of better ways to invest that sum. In the process of developing a contingency plan, this small business improved its operating procedures and has realized a return on the time and effort invested in contingency planning—even though disaster has, thankfully, not struck. Your small business can, too. With that point in mind, let's consider a contingency plan for proper handling of business mail.

BUSINESS MAIL PROCEDURES

Since letters tainted with the deadly bacteria anthrax were delivered through the U.S. Postal Service beginning in early October 2001, concern about the safety of our mail has prompted many businesses to reconsider their procedures for handling incoming mail. Public health authorities have confirmed 18 anthrax infections to date, including 5

fatalities. Five individuals in Florida; the Washington, DC, area; New York; and Connecticut died from inhaling anthrax spores contained in letters. Two of the victims, women in New York and Connecticut, appear to have contracted inhalational anthrax via cross-contaminated mail. We would like to remind our readers that the chance of contracting anthrax from cross-contaminated mail, according to Dr. Jeffrey Koplan, director of the Centers for Disease Control and Prevention (CDC), is "very low; the mail is, by and large, very safe."

Nevertheless, the incidents of anthrax infection by mail delivery have caused fear and anxiety in many workers who must handle postal mail. We believe that better information about the risks, as well as sensible practices for handling the mail, will alleviate much of the anxiety. In this chapter we present some basic information about what anthrax is, how it is transmitted, and how anthrax infections may be treated. We then present some suggestions for more efficient mail handling to reduce the flow of unnecessary mail and procedures for handling mail delivered to the office.

Background Information about Anthrax

Anthrax is an acute infectious disease caused by the spore-forming bacterium *Bacillus anthracis*. Anthrax most commonly occurs in animal livestock, such as cattle, sheep, and goats, and as such is most common in agricultural regions, such as South and Central America, Southern and Eastern Europe, Asia, Africa, the Caribbean, and the Middle East. Human exposure to anthrax usually occurs by occupational exposure to infected animals or their products. Transmission of anthrax to humans occurs in one of three ways:

- **Cutaneous (through the skin) exposure.** *B. anthracis* bacteria spores can live in the soil for many years, and humans can be infected with anthrax by touching anthrax spores from infected animals.
- **Inhalational exposure.** Exposure may occur by inhaling anthrax spores from contaminated animal products.
- **Gastrointestinal exposure.** Exposure to anthrax may occur by consuming undercooked meat from infected animals.

It is rare to find anthrax-infected animals in the developed world. Anthrax is more common in developing countries that lack established

veterinary health programs. The 18 incidents of anthrax that occurred in the United States from October 2001 were cases of exposure to weaponized anthrax, or very fine, aerosolized anthrax spores produced as potential agents in biological warfare. Hundreds of thousands of fine anthrax spores were placed in envelopes and mailed through the post to congressional leaders and individuals in broadcast media. The investigation to date suggests that the anthrax-tainted letters may have all passed through two post offices.

Symptoms of anthrax infection generally appear within seven days of exposure. The symptoms vary with the means of exposure:

- **Cutaneous exposure.** When the skin comes into contact with anthrax spores, the affected area initially resembles an insect bite and within one or two days of infection, an ulcerated lesion develops on the skin. The lesion typically has necrotic (dying black) cells in its center. Swelling may occur in the lymph glands adjacent to the affected area. With antibiotic treatment, fatalities are rare in cases of cutaneous anthrax exposure. About one in five untreated cases results in death.
- **Inhalational exposure.** Following inhalation of anthrax spores, symptoms similar to those of an ordinary cold may develop. Within several days of exposure, the symptoms include severe breathing problems, possible chest constriction, and shock. Inhalational exposure to anthrax is almost always fatal, unless postexposure antibiotic treatment is initiated.
- **Gastrointestinal exposure.** Following ingestion of anthrax-contaminated food, the symptoms of exposure may be similar to those of inflammatory bowel disease: acute inflammation of the gastrointestinal tract (from the mouth to the esophagus to the stomach and to the large and small intestines). The initial symptoms include loss of appetite, nausea, vomiting, and fever. In the hours and days following exposure to anthrax, more serious symptoms develop: severe abdominal pain and diarrhea, possible bloody diarrhea, and vomiting. One-fourth to one-half of cases of gastrointestinal exposure to anthrax result in death.

Anthrax is not contagious; that is, it cannot be transmitted from infected person to person. The U.S. Food and Drug Administration has stated that there is no known case of anthrax infection from blood donors who may have been exposed to anthrax but were in good health.

Standard blood collection procedures screen for donors with symptoms of illness that would suggest anthrax infection.

Diagnosis of anthrax infection is made by isolating the *B. anthracis* bacteria from the blood, skin lesions, or nasal secretions. The treatment for anthrax infection is a 60-day course of oral antibiotics, such as Cipro®. Anthrax infection can be prevented by vaccination. However, the CDC does not recommend vaccination, except for those individuals who work directly with anthrax in research laboratories, those who work with imported animal products without adequate protection against contact with spores, those who handle possibly infected animal products in developing areas of the world, and military personnel who may be exposed to anthrax as an agent of biological warfare.

The CDC also advises against prophylactic antibiotic treatment; that is, taking unnecessary antibiotics in the absence of a confirmed anthrax exposure. Frivolous use of antibiotics reduces the effectiveness of the treatment. The CDC has announced that, in the event of a mass exposure to anthrax, the federal government has in place a plan to deliver mass quantities of antibiotics to the affected communities within 12 hours of the reported exposure. While public health officials advise against unnecessary vaccines and antibiotics, we advise against processing unnecessary mail.

Reducing Unnecessary Mail

Reducing the volume of mail to your business site reduces the volume of letters and packages that must be screened by your mailroom. But, quite apart from concerns about mail safety, there are other pragmatic reasons for filtering unnecessary mail to your business site. If you often feel overwhelmed by the volume of messages reaching you, you are not alone. The Institute for the Future reported that 71% of the workers they surveyed felt stressed by the amount of information they receive each day: on average, 200 messages per day. Sixty percent of workers surveyed reported feeling "overwhelmed" by so-called "info-stress."[1] As a member of the small business community, your resources and your time are precious. Filtering out unnecessary messages frees your time for other, more productive work. I (Donna) remember receiving a deluge of mail solicitations (and telephone calls) after registering my business with the county clerk's office. The volume was excessive, and I resented the unwanted intrusions. Several of the solicitations related to fraudulent copier sup-

ply schemes, which I reported to the State Attorney General's office. The deluge resumed when I obtained telephone service for our business. I find it particularly irksome to return from a business trip and waste time sorting through junk mail.

Actions that you take in the ordinary course of work can invite junk mail to your business. These include completing warranty cards for your office equipment; subscribing to newspapers, magazines, or professional journals; filing a change of address form with the post office; listing your business telephone number; or ordering products via the mail or the Internet. We don't wish to exaggerate the risk: none of the reported incidents of anthrax exposure that occurred following the terrorist attacks of September 11 involved mail solicitations from direct response marketers. However, because such marketers seek to avoid having their solicitations discarded before being read, they often disguise the origin of their letters, thereby increasing the mail you may have to treat as suspicious. Our recommendation is that you filter it out as best you can.

The first step is to contact your local direct marketing association. Send a letter to the local direct marketing association indicating that you do not wish to receive any direct mail from its members. In the United States, write to:

Mail Preference Service
Direct Marketing Association
P.O. Box 9008
Farmingdale, NY 11735-9008

In Canada, the address is:

Mail Preference Service
Direct Marketing Association of Canada
1 Concord Gate, Suite 607
Don Mills, Ontario
M3C 3N6

In the United Kingdom, write to:

Mail Preference Service
1 Leeward House Plantation Wharf
London SW11 3TY
England

You also may write to these same addresses and address your inquiry to their telephone preference service and request that your business telephone numbers be removed from their telemarketers' lists. Be certain to include your business name and addresses of all of your offices or facilities in your letter. As previously stated, none of the incidents of anthrax exposure following the September 11 terrorist attacks were related to direct mail solicitation efforts. However, in our experience, direct marketers often conceal or disguise their addresses in an effort to persuade you to open a solicitation that you might otherwise discard. We also have observed that many direct marketers include free gifts in their mailings, such as free personalized pens, notepads, and other inexpensive items. These gifts increase the bulk of the mailings and may appear as "suspicious" mailings.

The next step is to write to the major sellers of mailing lists. These agencies collect data, such as business names and addresses, and re-sell them, over and over again, to their clients. We recommend that you write a letter, include your business name and address(es), and ask to be removed from their databases. The four largest database vendors to whom you should write are:

Metromail
List Maintenance
901 West Bond
Lincoln, NE 68521

R.L. Polk & Company
List Compilation
6400 Monroe Boulevard
Taylor, MI 48180-1814

Database America
Compilation Department
100 Paragon Drive
Montvale, NJ 07645-4591

Donnelly Marketing Inc.
Database Operations
1235 North Avenue
Nevada, IA 50201-1419

One ancillary benefit of having your business removed from the marketing databases is the reduced embarrassment of inappropriate mail being sent to you at your place of work. I (Donna) will never understand why one well-known company sent me lingerie catalogs at the office, having obtained my business address from a marketing database! How many women owners of small businesses wish to receive such catalogs at the office in the presence of their clients and employees?

The next step to reducing unnecessary mail is to write to each of the major credit bureaus and advise them of your wish not to be contacted. You may need to include your taxpayer identification number in your

letter for your business to be identified and removed from active data lists. Call the bureau in advance of writing your letter to determine their current procedures. The three major credit bureaus are:

Equifax
P.O. Box 105873
Atlanta, Georgia 30348
Telephone (800) 685-1111

TRW
P.O. Box 949
Allen, Texas 75002-0949
Telephone (800) 422-4879

Trans Union
P.O. Box 390
Springfield, Pennsylvania 19064-0393
Telephone (800) 521-4019

Finally, you should contact each of the companies with which you do business and advise them not to sell or rent your business name or address. We have written to the publishers of each of the trade journals to which my company subscribes and requested that they not make our name and address available to other parties. This has decreased the volume of our unnecessary mail dramatically. You must be vigilant because this is an ongoing process. When you, or any of your employees, complete a warranty card or order a product through the mail, you must be certain to include a note advising the vendor not to sell or distribute your name and address. These steps should reduce the volume of mail to your place of business.

As a small business owner or employee, you may face the opposite problem: how do you ensure that your direct mailings to potential customers are not ignored? In the year 2000, $528 billion worth of sales were made through mail order in the United States alone. The anxiety that resulted from the delivery of anthrax-laden letters may cause the simple act of opening an envelope to provoke fear. You can take the following steps to assure the recipients of your mailings that your letters are secure:

- Identify your business as the source of the mailing. Be certain to identify your business through the return address. Present a pro-

fessional appearance with appropriate typeface on your mailings. Include your company logo on the envelope.

- Consider using a postal meter to stamp your mailings. In addition to saving you unnecessary trips to the post office, and the occasion to overpay your postal charges, metered mail is more likely to be opened and reviewed than stamped mail. This is because metered mail is more easily traced and therefore less likely to be used to deliver tainted mail.
- Eliminate anything from your mailings that could produce bulk or an uneven appearance. A flat letter is less likely to arouse suspicion in the recipient than an uneven, bulky envelope.
- Use clear window envelopes showing the recipient's address. A transparent envelope is less likely to contain an unwanted substance. Or you may use postcards to contact potential customers. You also may choose to notify potential customers by advance postcard that a product sample is coming, for example, so that they expect a bulky package from you.
- You may wish to apply a seal across your envelope flaps to assure the recipient that the envelope has not been tampered with since it left your place of business.

Finally, to protect the reputation of your business, ensure that your outgoing mail facility is secure. Conduct careful preemployment reference and criminal background checks to ensure that those who join your company will be of good character and not likely to misuse your company's mail facilities. Make certain that only your employees have access to your mailroom. We visited the offices of a Manhattan law firm that propped open the door to its mailroom after hours because the personnel who received courier packages at all hours of the evening did not wish to miss a delivery whenever they stepped away! The mailroom opened onto a public corridor near the elevator bank of a large Wall Street office building. Don't do this. Be certain that your business facilities are secure.

Handling Incoming Mail

Make certain that you and your employees are alert for suspicious packages and letters delivered to your place of business. The U.S. Postal Service advises us that suspicious mail includes mail that:

- Displays a powdery substance.
- Is unexpected or sent by someone who is not known to you.
- Has incorrect postage, a handwritten or inaccurately typed address, incorrect titles or a business title without a name, or misspellings of common words.
- Is addressed to someone who is no longer with your company or is otherwise out of date.
- Has an unusual amount of tape sealing the mailing.
- Gives off an unusual odor or displays stains.
- Has no return address or one that cannot be verified as legitimate.
- Is of an unusual weight or shape, possibly lopsided.
- Is marked with restrictive endorsements, such as "personal" or "confidential."

Do not open, shake, or empty the contents of any suspicious envelope or package. Contain the suspicious piece of mail by placing it in a container, such as a plastic bag, to prevent its contents from leaking. Leave the area where the suspicious mail is contained and advise others, perhaps by posting a sign, not to enter the area. Next, wash your hands with soap and water to prevent spreading any noxious substances to your face. Be careful not to rub your eyes or touch your skin until after you have washed your hands. Contact the police and your building security team and advise them of the suspicious package for their further investigation. Give the police the names of the other people who were present when you came into contact with the suspicious mail. Should the mail be tainted with anthrax, all individuals in the area when the mail was delivered will likely have to be tested for inhalational exposure to anthrax.

The procedure we have just described was the one followed by aides to Senator Patrick Leahy when a suspicious letter was delivered to the senator's office. The envelope was contained and then removed from the senator's office to a government laboratory where it was opened, and the contents tested. This is the procedure that you should follow in the event that a suspicious piece of mail is delivered to your place of business. Be certain that all of your staff are instructed in the identification and response to suspicious mail.

If a piece of mail escapes your screening procedures and you open it, what should you do if the mail contains powder? The first response is: *do not panic*. The powder need not be anthrax. Unfortunately, follow-

ing the events of September 11, the occasional prankster has sent baby powder in the mail to provoke fear and anxiety in the recipient. We can tell you from our personal experience that we were evacuated from a New York City subway when a powdered substance was found in the subway station. The powder was, thankfully, not anthrax.

Once you have collected yourself, do not attempt to clean up the powder. Immediately contain the spilled contents with any available covers, such as a waste basket, or paper, or a piece of clothing and turn off any fans or ventilation units in the area. The idea is to limit the amount of powder that can become airborne. Leave the area where the powder is contained and advise others not to enter the area. Wash your hands with soap and water, again exercising care not to touch your skin or rub your eyes. Immediately contact the police and your building security team. Remove any contaminated items (such as your clothing and items on the desk where the mail was opened) and place them in a sealed plastic bag. This bag should be given to emergency personnel for proper testing and subsequent disposal. Shower with soap and water and remember to give the names of those individuals who were present when the powder was released from the mail. Should the powder be identified as anthrax, those individuals will likely have to be tested for anthrax exposure.

I (Donna) worked at an investment bank where all incoming mail was subject to x-ray screening. We recently read that post offices that deliver mail to government offices are also irradiating their mail. Such costly technology is likely beyond the reach of most small businesses, but technological innovation has made other screening techniques feasible. Many companies now offer electronic document delivery. These businesses accept and open your mail (with many customers for whom to screen mail, it is presumably cost-effective for them to irradiate the mail) and then electronically scan your mail. Junk mail is discarded. All other mail is delivered to you electronically—you never touch the mail!

Stefan used this type of service long before anthrax-tainted letters were delivered to victims in the fall of 2001. Because he travels to Europe frequently, he finds it convenient to have access to his mail while on the road. It also helps him to pay his bills online, so bill payments are not delayed until his return, and his credit rating remains unblemished. You can find companies offering such services through the search engines on the Internet.

Internal Communication

Ongoing communication within your small business is vital. You must strike a balance between calming fears and staving off complacency. As the weeks and months pass, and the anthrax attacks of the fall of 2001 recede into the past, complacency will inevitably creep in. Staff may become less vigilant about mail security. Ongoing communication is essential to ensure the safety of your staff. Make certain that your staff understands proper mail handling procedures and provide periodic reminders. The most important aspect of communicating the proper procedures for handling mail is to address any fear and anxiety that may linger about anthrax infection.

IT INFRASTRUCTURE

I (Stefan) am experienced in managing large-scale projects, such as evaluating the IT strategies of global companies. But I also work with small business owners and individual professionals to develop their IT solutions. Small business owners often are apologetic about the nature of their problems, as if the work they present is not as prestigious or challenging as working with large global corporations. Actually, I enjoy working with small businesses because they are dedicated to their work and appreciative of some straightforward advice on how to grow their businesses without exhausting their limited IT budgets. It is gratifying to contribute to the realization of the dreams of small business owners and employees. It also presents its own unique challenges: how do you solve the problems at hand when you don't have the deep pockets of a large corporation to build and maintain your IT infrastructure? I find that this work gives me the opportunity to learn and to readjust my perspective, which is occasionally distracted when focusing on high-level corporate issues.

My first meeting with the president of a corporation or the owner of a small business usually starts with a casual conversation about the current state of IT technology. At today's pace of development, there is always something new to talk about. But when they start to tell me their stories, they express elements of frustration when they report to me that "we have spent thousands of dollars on our IT infrastructure, but when

I recently wanted to do . . ., it was tremendously difficult and I was just wondering if it has to be like that. That's why we want an independent assessment from you." When I hear such comments (and I frequently do), I know that something has gone terribly wrong between the businesspeople and the IT team.

Most businesses have an in-house IT staff or a relationship with an external consultant that has built their systems, and of course, such relationships are valuable and it is not in the interest of a small business to abandon such relationships in frustration. The IT team that built your system knows the overall system in detail and has made decisions based on the specifications that your business had provided to them. They may have been instructed to implement a certain feature "exactly this way." Should you terminate this relationship in haste and replace your existing team with a new IT solutions provider, you will incur additional costs and you will likely once again be disappointed with the results. Remember the expression from the movie *Cool Hand Luke*: "what we have here is a failure to communicate." It can be very frustrating for technologically savvy IT professionals to try to implement a systems solution at the direction of businesspeople who really don't understand the technical constraints or the inherent contradictions or unreasonableness in what they are asking. At the same time, it is disappointing for businesspeople to invest significant sums of capital in IT capacity and find that the result is not what they had anticipated. In such situations as these, what you need to do is to make sensible and yet powerful changes that will be welcomed as improvements without embarrassing or blaming the existing IT members for their decisions.

In conversations with small business owners, I often start talking about contingency preparations, and they respond with blank stares and tell me that this is not of immediate concern, and anyway, they are already well protected because they just bought this fancy network storage backup unit, or else they hired the same consultant that did the backup system for large corporation XYZ. But as I continue to examine their needs with my persistent questioning, they begin to understand my perspective. I believe that a good IT solution provides contingent capacity, is simple, and is easy to operate. Creating or reviewing for contingency includes analyzing the current infrastructure, determining how the system is used, understanding current and future needs from a high-level perspective, and observing if those needs are met and if they will be met in the fu-

ture. The exercise of developing a contingency plan opens the door for a productive dialogue with your IT staff, as well as with your customers, suppliers, and business partners, who should all be a part of your contingency efforts. The result of this dialogue will be, I hope, a simplified and streamlined technical architecture that leads to better, more cost-effective solutions, and additional contingent capacity. This is a far more effective solution to your business than mindlessly importing the solution developed for large corporation XYZ. Generally, the solution that was developed for a large corporation and then scaled down for use by a small business fails to yield the desired results.

Small business requirements for IT contingency and IT solutions differ substantially from those of large businesses. We often see good solutions that have been developed at large customers simply downsized and implemented in small businesses. But they are in most cases not cost-effective, not sufficiently flexible, and not easy to use in your day-to-day operations. And I am sorry to report that should you find your small business in disaster recovery mode, the system you imported that was originally developed for use by a large corporation will become an impediment to your recovery efforts. The good news is that you can learn from the mistakes of other small businesses that attempted to import solutions that were inappropriate for their needs, and develop your own, much simpler solution, at greatly reduced expense.

In developing a disaster recovery plan, businesses often put in place IT systems that anticipate and prepare for the worst-case scenarios, such as the total destruction of their business facilities, and assume that all less severe disasters are subsumed and automatically protected by the steps taken to protect against the worst-case scenario. In fact, I have read such advice in a number of general books about disaster recovery! This assumption generally holds true, but it should not be the basis of your contingency planning. Do you intend to initiate a full-blown disaster recovery action plan each time you experience a small deviation in normal operations? Do you think that is a cost-effective way to run your operations? In fact, it is much more sensible for small businesses to have a good solution implemented that deals efficiently with the most com-

mon "small" disaster types, such as human error, and therefore provides a swift recovery. Of course, you also want to have some protection in place against the worst-case scenarios, such as a severe terrorism attack, but it is unlikely that most of the readers of this book will ever be required to implement such recovery operations. Small businesses typically need a modest, cost-sensitive solution that deals with their specific daily operations issues, which typically means developing a solution that provides for immediate recovery from modest disasters, even at the expense of slightly extending the period of recovery from severe disasters.

This, of course, is a different approach than the one advocated by large-scale corporations. They need good solutions to protect themselves against severe disasters, such as terrorist attacks. In the case of such disasters, their very existence is at stake. Imagine the situation facing the IT teams of the large money-center banks in Manhattan on September 11, 2001. They have an enormous volume of financial transactions to process, so fast recovery from severe disasters is mandatory for them. You won't be surprised to learn that within five minutes, I could walk from my apartment to the backup facilities in Jersey City that were humming on September 11, taking over the responsibility of processing banking transactions from their Manhattan-based colleagues. At the same time, however, these large corporations don't expend much effort worrying about protecting against human errors, such as the mistaken deletion of a computer file. Should such human errors begin to interfere with their operations, they can simply correct the problem by mobilizing the manpower of their vast IT departments.

To find out what you as a small business really need to feel comfortable, and to make IT infrastructure a cornerstone of your business, you should start with finding good answers to the questions related to protect yourself against the six IT disaster types we presented in the Introduction. The following are some sample questions; you will probably have to add your own questions to this outline:

Human error: How do your employees store their data? Is a standard naming scheme in place? Do you have in place version control for documents? How do you share data between groups? How much do you want to invest in user training versus protecting data through more technology expense? How quickly must lost data be restored?

Equipment failure: Which are your most critical systems? What perfor-

mance do you require from each system? What are acceptable downtimes to your business in case of malfunctions? Which infrastructure elements need special protection? Do you have a dedicated budget for spare parts and equipment replacements?

Third-party failure: How essential is e-mail (and thus reliable Internet connectivity) to your business? How long could you work without your phone? How often do you expect power outages and how long would the outages be?

Environmental hazards: Did you check your offices for environmental toxins? Is your lighting system compatible with your computer screens? How did you prepare for office safety against contamination by hazardous materials? Which systems must be available remotely if you were to leave the office right now?

Fire and other disasters: Do you have backups at a safe remote location? Do you have special equipment to detect fires and to automatically shut down your equipment? Is your staff aware of the emergency shutdown operations? Do you have fire protection containers for important or valuable items?

Terrorism and sabotage: What is your emergency plan? Will it ensure safety of your trade secrets? Are you secured against a targeted hacker or virus attack? How do you protect your business from any disgruntled former employees?

These are just a few sample questions to guide you in developing a longer checklist that is suitable for your own unique business needs. These are the questions you should ask yourself. Did you find some that caught your attention? Are you beginning to think about answers to these questions? As you continue to read, we will ask more questions, and even answer some of them.

The process of asking questions is often an eye-opening exercise for many small businesses. You will realize against which types of disasters you have adequate protection and against which ones you have inadequate protection. As you work through this exercise, you begin to see how your business processes and critical tasks are connected to your IT infrastructure, and how you can achieve a better link between critical tasks and information systems. You will be able to view your IT infrastructure with more confidence, advising your IT staff or consultants to targeted actions to improve specific processes and to respond in anticipation of certain scenarios.

Human Errors

Human error is, by far, the most common and most frequent cause of business disasters. By definition, human errors are unintentional, and because they occur randomly, we hope that the overall impact on your business operations will be negligible. Each of us has had the experience of developing a new document by revising an older document or by using a template. When we finish our work, we hit the "save" button, and immediately realize that we have just written over with new text an old document that we will need again in the future. The same is true when we reorganize our files to reduce the clutter we made in the last month and unintentionally delete a whole folder of important documents.

Unfortunately, there is no single simple solution. We have to expect that human errors will be made, and we must be able to protect our businesses from ourselves to the extent possible. I (Stefan) often notice that managers hope that their employees will be careful with important files, and when they inadvertently delete a file, they hope a backup file exists. I usually suggest keeping track of these events. If you do so, you will begin to realize that these errors occur with greater frequency than you thought. A CD burner is enthusiastically used for backing up data and then forgotten after a few weeks have passed. And the corrective action taken is most often less than satisfactory. In fact, we frequently have observed that the loss of a file is either not even realized or simply never reported, until someone runs nervously through the company asking if anyone still has a copy of a particular file. By that time, it is usually much too late to recover this file from backup systems and it would require more time to retrieve the deleted file than to create a new one. IT managers often have businesspeople making requests of them such as "Could you see if we still have a backup file of the presentation we gave to our most important client last year? I don't remember the name of the document, but I wrote it in the first quarter of the year." This is not an efficient use of anyone's time, and as a small business owner or manager you know that experienced IT professionals are too expensive to be used in this manner and you have too many other important tasks for them.

Small businesses need a solution that is a combination of user training and a backup mechanism from which users themselves can recover unintentionally deleted files. It helps both the users and the IT staff because the users no longer have to request the IT

staff to recover files for them, which can be needlessly time-consuming. And as a small business owner, you do not need to hire someone to operate the backup system in the event your staff needs to retrieve files.

User Training

It took me (Stefan) some time to develop a system for archiving my files that works for my business and allows me to recover work that was done years ago. I have about 10,000 files compressed into three gigabytes of data. I am sure you can appreciate the volume of documents and files that a small business creates, so you understand the importance of retrieving your data. The future of your business depends on the quality of its information resources and the timely availability of any data needed.

Now imagine you have hired a new employee. Unless you have some guidelines in place, how do you expect this new person to store documents in a way that another employee can easily retrieve two years later? Training your new and, if necessary, your current employees will not just simply be a computer training exercise, but it will also raise the awareness of how your employees should support the contingency plan. We recommend that you provide at least some instructions to your staff on:

- Storing data on your computer system (and how *not* to store data).
- Sharing data among work groups.
- Naming files in progress and naming of files for archival purposes.
- Using version control for documents.
- Creating logical links, for example, hyperlinks, between documents.
- Archiving files and initiating immediate snapshot backups.
- Retrieving files from your backup system.
- Shutting down your computer system safely.
- Deleting files.

This project will require an investment of time, and therefore it has a cost associated with it. But once you adopt agreed-upon practices for data handling, they will soon become standard procedure and your existing staff will cross-train new employees. I am certain that after a few months you will realize the benefits of establishing these procedures.

When I (Stefan) advised Donna on how to establish such a system, she reported within two months that her business spent less time retrieving, changing, and filing documents. It was particularly helpful for her business, because she works with overseas clients. Differences in languages and practices can result in some creative document naming (and some hair-pulling exercises trying to imagine which keyword would help to locate a document when the author of the document speaks a different language!). Once you adopt these practices, your business will be able to easily identify inconsistencies and correct them much more quickly. Group collaboration will become much easier. Isn't that what your small business is all about—bringing people together to accomplish a shared goal?

Data Backups: Part 1

You have data that must be stored safely. Most of it is mission critical. The types of digital information may range from the product documentation created by your employees to the details of key customer accounts, business contacts lists, sales databases, and e-mail correspondences, just to name a few. For yours as well as for many other companies the competitive advantage resides in these information assets and the trained staff who can work with them. But these staff are the very same people who make mistakes from time to time. User training can do only so much. User errors will continue to happen.

Making data backups regularly is your second line of defense after you have trained your users. But these are not the type of complete system backups that are made as a precaution to equipment failure. Those we will discuss later. The backups that are needed here must address the needs of the users, and therefore must be done more frequently and initiated by users themselves. Restoration also must be simple and quick. As a small business, you cannot afford long downtimes or call an IT specialist for retrieval of your files when an important file has been mistakenly altered or deleted. Just the fact that it was important indicates that it is most likely used and modified frequently.

Tapes as a backup medium are impractical for this purpose because they store data sequentially, meaning data cannot be accessed directly; thus, recovery time is fairly long. It can easily take hours to find a particular file on a large tape. Other removable media, such as diskettes, ZIP

disks, or CDs, allow the direct access of data. Diskettes are limited in their storage capacity, and as such, usable only for small projects. ZIP, CD, and DVD drives have much higher capacities, but still, you rely on the user to make backups regularly and correctly. And users can make mistakes here as well. Nothing is more disappointing than finding out that your employee's backup did not store the important files correctly.

In any case, users expect automatic backup of their work and rightfully consider anything short of that a needless annoyance. In addition, you need to be aware that creating backups on removable media could raise a security concern because employees could take large amounts of confidential data with them without leaving a trace. In fact, if data security is a major concern for you, you should restrict access to all high-capacity media drives and monitor your online data traffic in and out of your company.

You will need a backup solution that allows you to make quick backups with easy retrieval of files by each individual user. If you look into the market for backup storage systems, there are about 50 companies supplying this market. Most specialize in enterprise size solutions, but some of them also offer downsized solutions from their larger cousins to small businesses. They are indeed fast and reliable backup solutions, but they come at a steep price that would leave a large dent in your IT budget.

In any case, you should select an adequate backup system that fits your requirements as a small business in several ways. It must:

- Provide the data security that you need, either on-site or off-site.
- Be able to handle to handle your typical amount of data within time frames acceptable to you.
- Provide a retrieval time suited for the disaster type case that you are trying to address.
- Provide a cost-effective solution for your targeted recovery time.

For small businesses, in most cases, you do not need fancy network storage hardware, or the latest gizmo in online storage technology to provide an adequate contingency backup solution with fast retrieval possibilities. Imagine that you would like to make a snapshot backup every hour of all user data files. If the amount of user data that has to be transferred each time is less

than about 10 gigabytes, and this is true for the wide majority of all small businesses, a simple PC with a couple of large hard disks and a basic network configuration will do just fine. In fact, you could even save on buying another operating system, and simply use a free UNIX operating system, such as Linux or FreeBSD, and use their built-in methods to share its file systems with other operating systems. If you configure this machine for input/output (I/O) performance, you have essentially the same network storage solution that is otherwise sold for at least three times the price.

With regard to online storage solutions, you send all your data to a safe data center located off-site. Preferably, your data should be encrypted and secured if you are using the Internet for this purpose. The use of such online storage solutions looks appealing at first glance, and is often an elegant solution, especially if they are directly supported by the operating system's drag-and-drop windows (e.g., Windows 2000 or Windows XP Professional). Be aware that you will pay a fee per month or per year for the actual amount of storage used; your bottleneck in transferring the data will be your Internet connection, or the Internet itself. And then there are often limits on the amount of data you can transfer in and out of such a facility per month. By the way, similar limits will most likely also apply for your Internet connection, especially if you are using a digital subscriber line (DSL) or a cable modem. A small business should consider if online storage solutions really satisfy its needs, and compare them with the alternatives that we propose in this book.

There are many different software packages in the market that allow you to create a backup of your data independent of the final storage medium, if it is another hard disk, a remote location, or a tape drive. A simple backup utility is already included in Windows 2000 or XP Professional, and you may buy other software packages separately. However, for the amount of data typically handled by a small business and using it for the purpose to recover from user error, we feel that special backup software is not necessary. You want to avoid many of them because they use proprietary backup file formats, and you do not have the large business facilities at your disposal where you can ensure that you will still be able to read your backup file format after five years has passed.

To create backups of user data, we suggest that you first familiarize yourself with any easy to use file synchronization tool. A variety of such

tools exist, some commercially available, others integrated in operating systems or simply for download as shareware from the Internet. The way these utilities work is that they simply scan your local files and all your files on the backup system and then determine which files need to be updated because they have been newly created, modified, or deleted. It is the same method used by mobile devices running the Palm operating system, Pocket Windows.

After the initial run (which might take some time if your overall data sets are large), these tools are usually very fast. They scan, for example, 10,000 files with three gigabytes total size in less than 10 minutes, and replace 100 altered files on a backup hard disk in less than one minute. The file synchronization can be triggered by the user anytime. In addition, an automatic update every hour or every night should be scheduled. You can keep as many of these automatically created snapshot backups as you have disk space on your backup system.

If all users store their data on a file server, run a backup in the same manner between the file server and the backup system. However, we like to stress that usually no live file server for user data is needed for small businesses until you reach a certain size or data complexity. It is sufficient to keep data locally on each PC, and then to consolidate these data by file synchronization, on- or off-site, on a file server that must be available at certain times. Since the data will be stored at two locations, no further backup of that file server is needed for this disaster scenario. You will be surprised at the cost savings that result from this simple solution.

The backup file system should be configured to provide all backup data with appropriate access rights to the users on the network, so that everybody can access and rebuild the data at any time. For ease of use, you can even make all backups available through your web browser, but again, review data access for adequate data security. And by the way, the availability and continuous usage also ensures implicit testing of your backup system, although you will want to methodically check it out once in a while.

Equipment Failures

Sooner or later, a component of your IT equipment will fail. (Fortunately, equipment failures occur less frequently than human errors.) Sometimes you encounter an even more frustrating scenario: an unreliable computer

that periodically malfunctions. This is a fairly common scenario: about half of data losses on desktop computers can be attributed to data corruption on the hard disk, caused in equal measure by physical hard disk surface damage or software glitches. In one-third of the cases, data are lost due to interruptions in the power supply. In about 10% of the cases, data are lost from desktop computers due to overheated parts, because fans inside the computer were clogged by dust or otherwise malfunctioned. This happens more frequently in dusty or carpeted rooms. The remaining 10% of the cases of data losses from desktop computers can be attributed to other causes, such as processor and board failures.

For our present purposes, let us assume that such an event is localized; this means that only one system is affected at any given time. Later in this section, we will discuss complete system failures, including the total destruction of the system. We include in this category equipment failures that were originally caused by human error. Imagine that, in the process of repairing a broken lamp, you accidentally pull the computer plug. Afterward, the computer no longer boots because a major data corruption on the hard disk occurred when you mistakenly pulled the plug.

It is possible to create nearly perfect protection against system failures. This can go as far as building so-called high-availability (HA) configurations that in the extreme case call for guaranteed continuous operation and availability. This could be realized with two or more computers that monitor each other, and in the event of malfunction of one of them, the error is automatically detected and corrected and the defective computer is then shut down. These setups are used for critical trading systems, and the space shuttle has five computers in an HA configuration.

However, short of launching a space shuttle, or running an expensive financial trading operation, HA setups for typical continuous availability requirements are not cost-effective. These configurations are expensive to set up and to maintain. It is unlikely that your small business has such requirements. But you may have systems that require 24x7 availability such as, for example, revenue-producing websites and other e-commerce applications. Many companies would consider it desirable to also have 24x7 availability of their e-mail systems. We strongly recommend outsourcing such systems to a large data center. They can do the job for you in a much

more cost-effective manner than a small business ever could. They are experienced in professionally managing hundreds, sometimes even thousands, of servers under nearly continuous operating conditions.

E-mail is so often included as a critical functionality because it has become one of the most valuable resources for small businesses. In particular, businesses that have done traditionally most of their communication via regular mail or mail pouch now prefer to use e-mail for daily, informal communication and the exchange of ideas. Just think about, for example, law offices. A couple of years ago you would have visited your lawyer to discuss a contract. Today, you discuss these items efficiently via e-mail. If you are not a company that is doing business in the IT arena, like this example of the law office, and you have to call a third-party service to fix your computer system, you should consider outsourcing your e-mail operation to professionals who ensure its proper functioning around the clock.

For any IT systems that you will maintain inside your business, there are methods to improve the contingency against equipment failure. To begin, rank your systems and associated work flows into the categories of "critical," "important," or "optional" according to the following scheme:

- **Critical:** Systems that directly support your core business operation. For a small business, these systems should be outsourced and operated from a data center, but you might have very specific reasons (such as concerns about data security) for wanting to keep them in-house and you are willing to accept the occasional lack of availability to keep costs down. Examples of systems you may prefer to maintain in-house are your client relationship management system, your company shared documents database, and your internal web server. Your goals include system availability close to 24×7; downtime less than one hour during business hours; and data restoration capability of complete and immediate access on backup server during business hours.
- **Important:** Systems that provide important add-on services to your business operation, such as your meeting, scheduling, and calendar system or payroll and accounting. Your goals include system availability during regular business hours; downtime less than one

to two days; and data restoration capability that is complete, with backup data availability on the same or next business day.

- **Optional:** Systems that make your daily activities more efficient, such as scanners with text recognition software or video conferencing systems. However, no vital information is stored on such systems. Your goals include system availability usually operational during business hours; downtime less than three days or uptime as requested; and data restoration capabilities that are not required, but possible on special request.

You probably already have a good idea in which category each of your computer systems would fall. You are now ready to make a direct comparison and assess the trade-offs between system failure and contingency measures, which should give you a clear idea on the required budget and manpower to protect each computer system appropriately.

Note the importance of simple regular maintenance on your equipment. This is an effective measure in avoiding failures that are most often caused by truly trivial circumstances and therefore create more hassle than actual damage. For example, components like monitors, keyboards, and mice often fail because they are directly exposed to human beings who sometimes spill coffee over them. Fortunately, they are easily exchanged as long as you have replacements available. You also want to open each computer from time to time. Fan inlets that are clogged with dust do not allow sufficient cooling of the internal components. This can quickly lead to overheating. Another warning sign of pending equipment failure is grinding noises from fans or hard disks.

Data Backups: Part 2

The backup strategy for equipment failure differs from the strategy for dealing with human errors introduced in the last section. With respect to contingency for human errors, the priority was immediate accessibility of data, preferably by the users themselves, and brief retrieval and restoration times for individual files. For equipment failure contingencies, the goal has shifted to minimize the total time that will be needed to restore the full functionality of the affected system.

Critical and important business systems must be protected by creat-

ing a system backup. The user data will be retrieved according to the simpler backup method presented in the last section of this book. Again, we must select the appropriate backup media for this purpose. In this case, we no longer seek quick retrieval of data, preferably by the user, but a complete backup of a computer system. Depending on the number and average system size of computers, tape can be beneficial because of its low unit cost per megabyte of stored data. If we compare the costs between the different storage media and assume that the cost of storing one megabyte on a diskette is normalized to one, storing the same megabyte on a ZIP drive is about 50% less expensive, 90% less expensive on JAZ drives, 99% less expensive on hard disks, and 99.9% less expensive on tapes. However, this picture changes when you take into account the cost of the actual hardware for the media drive. Fast and reliable tape drives are expensive, and unless you measure your data storage requirements in hundreds of gigabytes, which would be unusual for small businesses, high-capacity hard disks are close to an optimum between cost-effectiveness and quick data retrieval.

We often use a backup system with large disks to store complete images of the system partition. The advantage of doing so is the instant availability of this image anywhere in the network should the system ever fail. There are a variety of software tools in the market that provide exactly this disk-to-image functionality. Disk images are only dependent on the file system being used, which means that the data format is not proprietary to specific software.

Since your backup system itself becomes a critical part of your operation, hosting two different backup data sets, you should consider installing a RAID (redundant array of inexpensive disks) system. You simply add a second hard disk and connect both the old and the new drive to a RAID card, which is available at low cost. Configured properly, the operating system recognizes the two drives as one logical drive and any data written to that drive are written to both disks at the same time, effectively mirroring all data. Actually, if you use one of the free UNIX operating systems, like Linux, on your backup system, you can use the software RAID solution that is included for free. It is more than sufficient for a backup system.

The mirroring functionality gives you protection against hardware failures. But remember that a mirroring RAID system does not protect you from data lost due to human error. If you delete a file, it is deleted

on both mirrored hard disks. If you are concerned about human error as well, you should simply partition the logical hard disk into three areas, one for the operating system, and two partitions of equal size, one for user data, and the other as backup of the user data partition. Periodically, or on demand, you can use a file synchronization tool to update the backup data partition. Now you are storing each user file four times on two disks.

It is a low-cost solution that should give you more confidence about storing data on your desktop computer. Of course, the computer could be stolen or destroyed in a severe disaster. We will come back to this topic later in this book when we examine more severe forms of disaster. For our present purposes, we suggest that you could make the mirrored additional hard disk a removable drive and take it home with you each night to provide a readily available backup in the event of severe disaster. It will not be necessary to reinstall a disk should one of the hard disk drives fail because replacing the defective disk with a new one will automatically trigger a copy from the old disk to the new disk until the data on both disks are again the same. This process is easy, but can take hours to complete if the disks are large.

If this RAID method appears to be overkill with regard to your contingency requirements, another method is to use a single additional disk and copy data from the main disk to that additional backup disk using the same file synchronization or disk-to-disk backup tools as previously described. The advantage to this method is that you would initiate the backup yourself after you are sure that the changes on your main hard disk reflect the changes you wish to make. You can even use these tools to create a backup directly on an external backup medium, such as CDs or DVDs. However, with these solutions you lose the on-the-spot safety of a RAID strategy. If the main disk fails, you will have lost all changes from the time you ran your last backup to the moment that main disk failed.

Don't forget to periodically back up your system partition. You might think that if it fails, it can be easily reloaded from the installation CDs. Think again. Within only one year, you probably install numerous patches and updates, software specifically for use by only that particular computer, and customized settings with regard to the actual computer usage. Recreating this environment when the goal is to minimize system downtime is counterproductive. Reloading the system from scratch could easily become a daunting and time-consuming task.

You need to make the backup of the system data to a separate hard disk, DVD, or other high-capacity storage media. Using CDs for this purpose no longer makes sense if the system occupies more than three gigabytes of hard disk space. You would need about five CDs for that task. It is not the installation from such CDs that is time-consuming, it is actually creating them. You would need someone to first burn the CDs and then test them to ensure functionality. This isn't necessary if you save your backups directly on hard disks. The process of putting the same recovery data on a backup system within your network can be automated and takes less then an hour at night with no necessary human interaction.

Always remember, the additional costs of a backup system will pay off handsomely if you have to make use of your backup system only once in its lifetime. We want to stress that trying to repair parts or recover data from defective hard disks rarely makes economic sense. You should just replace the faulty part and rely on your backups for restoration of data. Interestingly, though, manufacturers report that about 70% of the hard disks returned for repair under warranty are still in perfect working order, but their data structure is corrupted. So before you return a hard disk for replacement under warranty, try to reformat the disk first and run a thorough hard disk check.

If you send your disk to a data recovery service, make sure you understand the costs involved. The service typically charges a low fee to take an initial look at your hard disk, but data recovery work on your disk can easily cost hundreds of dollars, even thousands of dollars, if data forensic experts have to reconstruct files that have been deleted. Consider not only the cost, but the inconvenience of not having your data for a couple of days. Of course, there is also a potential security concern when you send your hard disk to others.

One last piece of advice on this subject: if you have to recreate a system disk from the stored image on the file server, you will need to buy a new disk. Try to purchase the exact same model disk from the same manufacturer. If you choose a hard disk from another manufacturer, you need to be aware that hard disks vary slightly from manufacturer to manufacturer in size, even if the overall given size is the same. Copying the disk image back to a disk that is too small, even if only by a couple of megabytes, is not guaranteed to succeed.

Network Reliability

Network failures, especially for local area networks, are relatively rare. But a network is a good first test on how far contingency planning has progressed. When someone tells you that their network is completely protected and fail-safe, tell them that you will come over to their office and "pull the plug" on any one network cable. Observe their response!

Before you see network failures, you will typically first face network performance issues, like overloads of routers or switches, which clearly illustrate the need for good network capacity planning, especially if your network exceeds 20 users. If network reliability and performance issues are both of great concern to you, we recommend a practical approach, simply to "double-up." Every computer is equipped with two network adapters, and you have for each work station two network cable connections. You double your hubs, switches, and routers as appropriate. You may consider this overkill, and it probably is, but you should look at it this way: if it is done early while building your network, the additional costs will be modest. The standard CAT5(e) cable used for offices can by itself support two network and two phone connections, and you are building in a performance enhancement and a reliability upgrade at the same time!

With doubled network cabling and routers, you are now also able to have the routers automatically reroute your traffic through an alternative network path if the preferred route is down due to a failed connection. You also can use the mechanism for load balancing, but at that point you would probably need the help of an experienced network consultant. In any case, if you just think about this early in the process, such as when setting up a new office infrastructure, you can get all of this at little additional cost to your overall bill.

Of course, you should always have a carefully chosen inventory of spare networking components available, so that you will be able to quickly replace a faulty part. And if a network does go down, and you still have not outsourced your systems that need near 24/7 availability, you should install a network monitor that would automatically dial the numbers of the people that are assigned to handle the emergency. By the way, most of these units also monitor environmental conditions, such as loss of electrical power or room temperature as an indication of proper air conditioning. Some even can detect if smoke or water has entered the room and they can therefore be of great help in avoiding subsequent damage.

We recommend that you purchase stand-alone network components. It is generally not worth short-cutting expenses by not purchasing additional network equipment and instead configuring a computer as a router or print server, for example. You are building network functionality on a complex piece of equipment that is much more likely to fail than a comparatively simple stand-alone solution. This is especially true if the computer is also used for other network management tasks or even as a file server. And even if we do not consider actual hardware failure, we often hear complaints about performance issues, and we find printers that have severe configuration flaws, such as those that been connected via parallel ports on the file server. Serving this type of port requires a fair amount of processor power, something you definitely want to avoid on file servers.

Equipment Quality

If you are concerned about contingency, you want to have high-quality equipment. A few unreliable components can cause lots of trouble. They fail more often, they require frequent repairs, and they will eventually have to be replaced with a more reliable component.

I (Stefan) am often asked "Which computer should I buy?" The question is easier to answer if you are looking into some special market segment, like the large IBM and Sun computing and file servers or the Apple computers that are ideal for people who work in the design and media world. But when it comes to standard PCs, the answer is not as straightforward as you might think.

There are many sources where you can purchase new equipment. Standard PCs are available from large brand names, such as Dell, IBM, HP, Compaq, or Gateway, just to name a few, and there is a large market of lower cost brand name or good generic products. The real advantage of going with one of the big names is that you can rely on their support organizations if you ever have any trouble with your computer.

If you are looking for specifications on reliability, you will hardly find one for the computer system itself. The big companies market their products by technical specifications, such as processor speed, memory, and hard disk size, and often you need to be a specialist to determine why

two apparently identical systems are priced differently. Do you know the difference between the different memory systems, like SDRAM, DRAM, and DDR333, or packaging, like SIMM, DIMM, RIMM, and BGA, or that memory with DDR333 chips in DIMM packaging is referred to as PC2700? And what it all means to you for your daily work? Does it mean anything for reliability? We suggest that computer manufacturers watch the television automobile commercials. Cars are advertised not only for their horsepower and design, but also for their proven reliability.

You really want an answer to the question "Which computer should I buy?" If you go to a store and ask, you will get an answer, or at least the opinion of an individual ("I know this system from [large company] I worked for and, believe me, they do really make good computers"). To tell you the truth, the differences between the computers are marginal. The parts that are inside the box are pretty much the same in all computers. They are produced on a world market from a variety of large manufacturers. If you are in the market to buy a standard office PC or a simple file server, you should look for systems that have been labeled for use by small businesses. Many manufacturers offer these base systems at attractive prices. However, you need to know that they make their money with all the add-ons to that system, which you then purchase at a relatively high price—not unlike purchasing a car from the dealership! If you are looking for something truly specific, like a fanless super-quiet system, and you are somewhat PC technology-literate, you are probably better off looking for a "no-name." Actually, even with good no-names, reliability of the parts inside of a computer is of little concern, because if you really look inside, you will find that all manufacturers use more or less the same basic parts from worldwide suppliers anyway. And by the way, for the actual parts you will always find reliability measurements, like mean-time-before-failure (MTBF).

Do you really want an answer to "Which computer should I buy?" If so, we propose taking a different perspective. Think about the elements that you will interact with daily once the computer is on your desk: the screen, keyboard, and mouse. Here you will find quality differences, and if a part is defective, it is easily changed. So make sure that you always have some spare components available.

As for the keyboard and mouse, there are big differences in quality between a no-name and an actual branded product. From most inexpensive to most expensive, prices vary by a factor of 10 and more. If you ever experienced a mouse that constantly got stuck while you were trying to

finish an important presentation, you will appreciate an optical mouse. It is more reliable, more precise, and works on nearly any surface. For the keyboard, you should defer to the individual preferences of employees. A keyboard, and to some degree a mouse, can make a difference in someone's overall experience with a computer system. In the end, these are inexpensive purchases anyway.

As for the monitor, although they cost twice the price of comparable tube monitors, active matrix LCD displays over their lifetime will actually be the more cost-effective choice because they should outlast about two generations of computers and give a sharper picture that does not deteriorate over time. They use 70% less energy and can therefore provide extra time if you run on batteries. But you should be aware that there are differences in quality between LCD displays. The same manufacturer will produce a "consumer" and a "professional" version. The price difference is often marginal, but the professional versions are improved on important parameters, such as the contrast ratio, which should be at least 1:400 or higher, but in consumer products you will most often find only 1:300. If you still opt for a regular tube monitor, choose one with a dot pitch of 0.25 or smaller, a horizontal bandwidth of at least 70 MHz for sharpness, and a vertical refresh frequency at your preferred resolution of at least 80 Hz to ensure a flicker-free image.

The optimal amount of memory and disk space, as well as the processor clock speed, depends on your specific usage of the system. In general, however, most systems benefit from an upgrade of the video card. Poor video signals from original video cards can ruin your effort to obtain a clear image on your screen. Remember, no monitor will make a good picture from a poor input signal, and upgrading your video card is inexpensive. Since a fast processor can only perform well if it gets the required data from memory or the hard disk fast enough, plan to spend generously on memory (RAM) and a fast hard disk. Note also when comparing different systems that it is not simple to compare the processor frequency from one processor to another. Different processors with different architectures can have significant performance differences on certain tasks. For example, the PowerPC chip in Apple's computer is particularly good at handling operations on large bitmap files; thus it is well suited for the graphic design work it is often used for, although these chips run at about half the frequency as comparable Pentium chips.

For contingency planning, "equipment quality" as such is of little concern, because most brand name companies build their systems from parts often made by the same original equipment manufacturers (OEM). You need to make sure that the three things you work with every day—the monitor, keyboard, and mouse—meet high-quality standards. Keep your computer network as consistent as possible. The more similar systems you have, the easier it will be to rebuild your office infrastructure. You always want to try to buy or have at least four PCs that are identical. A greater number of identical PCs is even better, but small businesses typically buy about four PCs at a time. Always buy the latest generation processor. This should extend the lifetime of the PC for one additional year, and that usually compares favorably to the cost savings of buying last year's processor at a discount.

If you consider using laptops with a docking station at the office, keep in mind that laptops are generally more expensive and slower than comparably priced desktops. They are, however, very well suited for contingency planning, because you can simply take them with you.

For printers, an inexpensive printer will quickly become more expensive with increasing print volumes. Calculate the cost per page by considering the various ink and laser cartridges and compare the costs with your expected printing volume and you will find amazing results. So carefully review your requirements. If your printing output is mostly black and white copies, we recommend you start with a laser printer because it is generally more reliable than an ink jet printer. There is simply no liquid ink that can dry and clog up a print head. The laser printer should print at least 10 pages per minute and its cartridge should print 5,000 pages. If you like to print color occasionally or you need a second, inexpensive printer, then buy a separate ink jet printer.

We have reservations about buying systems that have many integrated functions. Over the past year, multifunction machines have become popular among small businesses. They are less expensive then stand-alone machines because they can share the housing, power supply, and so on. But it can become frustrating if such a machine malfunctions and must be sent away for service. You lose

all its functionality at once. You need to ensure that you have at least your basic everyday needs covered with simple, but reliable units, like an inexpensive black-and-white laser printer. Then a multifunction machine with color printing can be a fun addition for tight spaces.

Software Installation

Computer systems fail more frequently due to software glitches than to hardware problems. It happens all too often: the computer simply freezes and you need to reboot, potentially losing all the data in the documents you were working on. We recommend that you use only operating systems that have been proven stable and reliable in deployment for large installations (e.g., Microsoft Windows 2000 Professional or Windows XP Professional). The Apple Macintosh and many of the UNIX operating systems, either on their native platforms or in their Intel-compatible versions, are also very robust. They have become an economical solution for simple server functions, like file servers, web servers, and so forth.

In large businesses, PCs are deployed with a standard configuration installed. In small businesses, we often find PCs as they came out of the box, with various different software packages installed, most of them demo or light versions. Although this is done for marketing purposes, it is sometimes counterproductive to the reliability of such systems. In fact, it comes as no surprise to us when months later you suddenly introduce an incompatibility between new software that you just installed and a package whose name you had never heard of, but that was installed on your PC. Also check the compatibility of the software you are about to install with your operating system. We have seen systems that had to be reinstalled after a failed attempt to install incompatible software, such as installing Windows 95 software on a Windows 2000 machine. It is quite painful, but we can only recommend to small businesses that they also perform a clean installation of the operating system on delivery of the new hardware, and then install the applications that are truly needed, even if this initially requires more effort. But it will be beneficial in the long term, especially for reliability. It will effectively prepare you if you are growing and soon will have a network that would call for a "your-standard" PC configuration, with a standard office package and some standardized network and backup data access features.

We strongly recommend loading a system maintenance program. Make sure that the software you choose has at least the following features that you should be able to schedule for automatic run one or two nights a week:

- System virus scan and automatic updates over the Internet.
- Disk defragmentation.
- Thorough system inconsistency check.
- File system and hard disk error check.

These preventive functions will help to keep your PC in optimal shape, long before larger issues become significant and possibly interrupt the operation of the PC.

Third-Party Failures

You have made significant efforts to protect your business from human errors and from equipment failures. But you are not alone in this world, and your business is highly dependent on third parties providing a variety of services to you. There are direct IT services, such as your Internet connection, e-mail, and web hosting, which are provided via the Internet from a data center if you outsource these services, and of course there are the standard services, such as phone lines, electrical power, water, heating, and air-conditioning.

If you could, you would actually like to buy each service from two separate vendors, so that you have two companies providing you with phone service, another two companies providing you with Internet access, and so on. In theory, if one service fails, you would always have the same service from your other provider available. But that is only a theory.

When you buy services for your business, each supplier offers a whole list of service offerings and to make it really attractive, your salesperson will offer a nicely priced package deal. So a phone company would offer you Internet access together with their phone service, a cable TV company would offer you Internet access with your cable TV, and so on. Most throw in additional services, like e-mail and web hosting. Many people do not know that you can get add-on services by themselves, such as cable Internet access without actually having to sign-up for cable TV. In fact, you should carefully review if any type of bundling of services from one

provider is really worth the savings. Often it is not, and there is more built-in dependency than you would appreciate at first glance. For example, the e-mail accounts that accompany the service subscription are normally accessible only when you have been authenticated and are connected via that particular Internet service. Of course, the vendor will tell you that they are doing it to protect themselves from abuse of their mail services for relaying spam mail. But this is only partially true because there are many other methods, like separate authentication for outgoing e-mail or limiting the amount of outgoing mail from one e-mail account, which would have little effect on you but would deter individuals that would like to send spam mail to thousands of people. However, what your Internet service provider (ISP) is trying to do is to tie you, its valued customer, as much as possible to its services. This means that if your Internet access goes down, so does your e-mail. Only when you try to change your ISP will you realize how much they have managed to lock you in. Imagine this happens to you in a disaster situation: your ISP no longer offers services for whatever reason and suddenly you not only have to work on getting a new ISP, but you need to change your e-mail address as well. When you are in an emergency situation and responding to a disaster, you don't want to have your hands tied this way.

Choose your Internet service provider independently of the other services they provide in their package. You first want to make sure that the Internet service suits your needs. As for the provider's other offerings, like phone service, make them secondary services for your business and obtain a separate primary phone service contract from another provider. This is particularly true for e-mail and web-hosting service through your ISP. Use them for non-critical applications, such as a website for internal information that you make available with password authentication. Here you can post the latest marketing information that can be accessed by your sales staff on the road. Purchase critical services, like your e-mail and your sales-generating website, through a large independent data center.

When we speak of service that has failed, we do not necessarily mean total blackout of that service. In fact, most third-party services have clauses about reliability guarantees in their contracts, so the service itself rarely goes down. But the quality of the service provided is so poor that it is

practically useless to you. Then you have to fight with the provider to fix trivial problems like noisy telephone lines, slow Internet connections, surges in electrical power, or insufficient heating or air conditioning. Before you sign up with any company, you should try to meet the people in charge for your technical support when you enroll. They need to give you satisfactory answers to how they would resolve issues for you (and how quickly) and specify those guarantees in the contract. You also want to explore the possibilities of a test connection or visit one of the provider's existing clients and have your IT-savvy person check out important parameters, such as the bandwidth and latency for a planned network connection. You can then determine if it is within the range you need.

Before you start looking for an alternate provider, it make sense to first meet with a representative of each of the organizations that wishes to provide the service to you. They will sensitize you to issues that you had not appreciated. It is essential that you try to establish a good relationship with your contact at the third-party service provider. Attend any information sessions to which you are invited. They are a good opportunity to meet the senior management of that company in a casual setting. Mention to them that you are working on preparing a contingency plan for your business and you would like their recommendation on which provider you should use as a backup if their service fails—not that you assume it will, but just in case. It is a good idea to follow it up with a "thank you" letter expressing your interest in promptly completing your contingency planning.

You will achieve two results:

1. You should receive a letter outlining the contingency plans that your third-party provider has in place that will guarantee your service. The guarantee that you receive is usually somewhere between 99.5% and 99.9999%, equivalent to a few minutes per year.
2. Your provider will, reluctantly, recommend one of their competitors as a backup provider. They won't do it in writing, but they will tell you on the phone.

If you do not achieve those two results with your service provider, then switch if you can. It makes no sense to stay with them in the long run. In any case, you need to obtain contingency, meaning at least a second, maybe even a tertiary, service provider. And having a personal contact

with direct phone numbers is very important. If you are in disaster-recovery mode and need their help, you do not want to log a support request with their customer support desk thousands of miles away and hope for a prompt response by their local emergency team.

Again, if e-mail and web hosting are essential to your business, they should be hosted in a professionally managed data center. Outsourcing is not expensive. You can find simple web and e-mail services that cost less than $10 per month, and you definitely do not want to do your own constant network load monitoring, fault detection, and upgrade plans for scalability as your business grows. There are also some inherent advantages, because you might get some services at a data center that you cannot build yourself. For example, hosted e-mail services most often provide additional anti-spam measures that work by comparing e-mail that is sent to hundreds of e-mail accounts of different companies at the same time, indicating that it is some sort of mass mailing, most likely spam, that is then automatically blocked if you have requested this service.

In the case of a disaster, you want your staff focused on getting the business up and running. You do not want to think about moving services to get your website back up because your ISP has failed. In that sense, good planning and purchasing of services can definitely simplify your own disaster contingency plans. Make sure, however, that your service providers are well equipped to handle their own emergencies and can handle disaster situations at least as well as you can.

Phone Service

We have gotten used to reliable phone service. It is still one of the most used methods of communication. Remember that phone lines are not only used for oral communication. They are used to send faxes, to connect to the Internet via modem, or for credit card authorizations. After the World Trade Center disaster, many businesses suffered further losses of income simply because they could not use their credit card authorization machines when the telephone lines were down. One example is the Strand Bookstore Annex in Lower Manhattan, just a short walk from the World Trade Center. For many weeks after the disaster, this store and many other businesses as far away as Chinatown were unable to accept

credit card payments because its telephone service had not yet been restored. As you well know, customers who must pay in cash typically spend less than when they charge their purchases. It would be difficult to calculate the revenues lost to such businesses that had already lost revenues when they were closed during the period immediately following the disaster. Consider these other uses of phone lines to come up with an effective contingency solution.

In large cities, you can usually choose between several telephone service providers. But you need to make sure that you are not buying from two phone companies that are in fact each just reselling phone services from other parties. Otherwise, if that party has a problem, your service goes down, and your phone companies will simply refer you to the support desk of that third-party provider. It sounds ridiculous, but we found that when you evaluate phone service providers, let the providers show you their own physical phone connections into your building and make sure they are completely separate for the two companies you select.

Phone service failures are rare, but when they occur, you will need a backup solution. If you only have one phone company you can deal with, you protect yourself best if you have phone service through two different offerings of that company, such as analog phone lines combined with a digital line, such as ISDN or voice T1 circuits with 2, 3, or 24 simultaneous lines. In this case, analog lines would even work if your area is experiencing a power outage because the lines are powered by the phone company.

However, for small businesses it is rarely cost-effective to implement redundant phone circuits. If the telephone service fails, it is most likely due to a service outage, not to the actual hardware. But even if it is the actual hardware, because nearly every business executive has a cellular telephone today, the cell phone is the natural backup[2] solution for your land-based circuits. You should choose cell phones as your backup service of choice unless you are in a rural area with little cell phone coverage.[3]

The question is how to automatically connect land- and cell phone-based service so the cell phone service would take over if the land lines fail. The problem is that once the land lines have failed, it is not possible for you to forward land-line calls to the cellular phones.

The solution is developed by thinking in reverse. What you want to do is to buy a cell phone (of course, if you only plan to use it for contingency purposes, choose a calling plan that has the lowest monthly fixed costs) specifically for phone contingency purposes. You give out that number as your general contact business number. You program the phone in such a way that any incoming call is forwarded to your land-based business phone number when the cellular phone is switched off. If your land-based line fails, you simply switch on your cellular phone, and voilà.

This scheme can be easily extended to any number of cell phones and any number of land lines. You would simply configure both the cell phones and land lines in hunt groups, meaning that if the first number in the group were busy, the call would be redirected automatically and instantaneously to the second line, and so on. The last cell phone would be redirected to the first land line, which in turn would roll over to the second land line if busy. If the land line service failed, you would just switch on any number of cell phones that you needed. If you like this setup even for use during nondisaster times, remember to give out the number of the cell phone that you are carrying from the group of contingency cell phones so that people may call you directly, especially if they are used to calling your direct extension on the land-based system.

The last cell phone (or the last cell phone in your cell phone hunt group setup) forwards to a voice mail box. Again, you do not want to use any voice mail box that is provided with your land-based lines or your cell phones. You need one that has a different delivery mechanism than by phone because you also need to be prepared that the cell phones might stop working. In that case, any call would be forwarded directly into your voice mail box where you could listen to the messages, assuming, of course, that the forwarding mechanism still worked. Therefore, it is a good idea to publish your voice and fax service number on your letterhead and your business cards so that people have an alternative voice and fax number to reach you.

We strongly recommend that you sign up with a voice mail provider that delivers your messages over the Internet via e-mail. In fact, you should sign up with an integrated voice and fax service. This service often costs less than a regular phone line. Single providers of only voice mail or fax delivery via the Internet are usually not cost-effective.

Since the Internet has been designed to automatically reroute traffic if one or many paths no longer work, as long as you can connect to the Internet from somewhere, it is likely that you can receive your e-mails and hence, your voice messages and faxes.

In case both your land-based phone service and your cell phone service fail, your calls or faxes are forwarded to your integrated service number. You could even configure your system in such a way that it automatically sends you a short notification message with a summary of your voice or fax message to your cell phone or pager. At least you would know who called or who sent a fax. It is a service you will also enjoy during nondisaster times. It reduces unnecessary calls to your cellular phone.

You also might want to use your integrated service number for other benefits. If you use it as your public phone and fax number, you will prevent telemarketers and other people from calling you directly. They would need to leave you a message, and since the message is delivered by e-mail, you could screen it upfront. If it originates from a known junk message or fax source, you simply route it to your junk mail folder.

Another great thing is that these integrated services give you a local phone number or 800 number in any part of the world, with voice greetings in the local language. So people in Hong Kong can leave you a message as if you were a local business. And if you do not have Internet access, you can listen to your messages by phone. The system's computerized voice can even read you your e-mails over the phone.

Electrical Power

You probably will not have much choice with respect to utilities. You have to take the service provider that covers your city or county, although you can often choose which company supplies the electricity that they deliver. That doesn't change the fact that there is only one connection to the building. Whatever contingency you need in utilities during a disaster, you will need to provide yourself.

Electrical power is usually available at any time. Still, there are also quality issues, like peaks in voltage as well as micro-outages, especially in rural areas where you have large users of electrical energy. Because most IT equipment is sensitive, it is best to use a surge protector, even better

to use an uninterruptible power supply unit (UPS), which is usually a surge protector, together with a small buffer battery that would supply energy for about 10 minutes, enough to finish important work and to shut down the system. Most units support an automatic shutdown before the battery is completely depleted. Think about laptops as computers with a built-in UPS!

Some buildings supply self-generated backup power. This power is usually much "dirtier" than power from the outlet. Under these circumstances, you need to have a UPS unit, preferably one that is designed to smooth out a rough electricity supply. Most do.

During any power outage, one of the most limiting factors will be the fact that simultaneous failure of the air conditioning can lead to insufficient cooling of equipment, especially if it operates in a small space. It is therefore a good idea to keep track of the inside temperature of key equipment, to ensure that the environmental conditions are adequate. If the air conditioning for a machine room fails, all nonessential computers should be shut down. The essential equipment will be monitored and, in due course, will be shut down as well.

Internet Access

In general, a small business will most likely consider the following options to connect to an ISP:

- Dial-up via an analog or digital phone line.
- Connection via DSL or cable.
- Connection via a data circuit, usually a T-1 line, either dedicated or shared with other users.

Before we can talk about how to use these different services to establish good redundancy, we will go a little deeper into some specific technical details that you do not find advertised as such. Each vendor will only tell you the benefits of his solution and not how it compares with competing services.

The dial-up method through a regular phone line is the most basic means to connect to the Internet. The immediate advantage is that phone lines are readily available and can immediately transfer data. The drawback of the analog dial-up is the limited bandwidth. In general, consider

a 56-kbps (kilobits per second) modem as the bandwidth that you will probably never reach. Depending on the quality of the phone line, the actual connection speed is much less; in this case, typically around 50 kbps.

Phone companies use digital circuits with digital compression methods to optimize their usage of available bandwidth. With ISDN (Integrated Services Digital Network), a direct connection to the digital phone line is established. Two data channels of 64 kbps provide a total usable bandwidth of 128 kbps. Like an analog modem connection, ISDN is still a dial-up to a service provider, and thus it usually comes with per-minute usage charges if you exceed your monthly allotment. ISDN has been quickly superceded by higher bandwidth solutions, but this might be a cost-effective solution in rural areas where other data line services are expensive.

Most residential high-speed Internet connections are based on either cable modems or DSL. The data signals are overlaid through your cable TV or phone line without interfering with the primary signals. The main difference between the two is that TV cables are highly interconnected within the same building; thus, you share your high-speed connection with everyone else who is connected. In contrast, DSL lines are dedicated connections. However, this does not guarantee that your data are not eventually routed into a shared data network at your ISP. In fact, this is most often the case, and your ISP might hand the data to another ISP, which hands it on to another ISP, and so forth. Of course, that also can happen with a cable modem ISP, but we have seen it more often with DSL service.

The bottom line is that both DSL and cable modems provide fast Internet connections. But they do not guarantee data throughput. Performance will vary greatly depending on the load of the network segment to which your service is connected. You will often see service disruptions, especially during peak usage hours. ISPs often limit the maximum amount of data you are allowed to put through your DSL or cable modem Internet connection, simply to discourage users who are misusing the connection to host Internet services. While both services are generally reliable, there are occasional short outages and not the same uptime guarantee you get with true data connections. If the service goes down,

Murphy's Law states that it is just at the moment when you are sending your most important e-mail ever.

Dedicated data connections, such as T-1 circuits, are best if you rely heavily on your Internet connection. They have been around for a long time, and they provide solid data connections. You can obtain data service with a variety of up-time guarantees, but it is usually significantly better than DSL or cable. Of course, this comes at a price about five times higher than for DSL or cable connections at a comparable bandwidth. In rural areas, unfortunately, you also have to pay a charge per mile to the next data connection point of the telephone company. Sometimes you are asked to share a T-1 connection with several of your neighboring businesses, which could be a cost-effective option.

Even if you obtain a dedicated data connection with a high availability guarantee, if you really depend on the Internet for your business, as many small businesses do, you still need at least one more alternate connection. Data lines, as telephone lines, are susceptible to equipment failure due to ordinary events such as disruption by construction work. It has happened that data lines have been mistakenly cut by construction work on the street, leaving you vulnerable if no other third-party provider has its own independent cabling in place.

You need at least two methods for connection to create additional redundancy. In principle, you could use any two methods, but for practical purposes, you would always choose two comparable bandwidth solutions. As a third backup, it is always a good idea to have one or more analog phone lines reserved. But a word of caution: you do not want to connect your PC directly to an analog phone line and dial-up your ISP. You would create the risk of a security breach. Instead, you should use a separate dial-up modem, router, and firewall integrated unit that will protect your network and automatically share the access to all computers in the network.

DSL and cable modems are a good pairing for redundancy. In most cases, these services are delivered through two different access points in the building. The drawback is that cable modems are usually not available in commercial areas. For a small business it could be sufficient to have the DSL connection at work and the cable access at home, if it is

feasible for you to drive to your home when the DSL connection goes down.

We recommend most often a (shared) T-1 connection as the primary Internet service with a DSL as backup. You need to ensure that both services come through two different sources, meaning physical access points in the building and different network paths to the Internet backbone. In urban areas it is often the case that DSL service is routed somewhere at the phone company through the same connection points as T-1 lines. If there is a major disaster, both services are lost. If in doubt, add some analog lines from a different phone company or through your cellular phone, just to be safe.

In any case, to ensure adequate Internet service at any time, suggest that your Internet providers configure your line to ensure minimum throughput to certain sites, especially during peak usage of the system. All other less important traffic is routed through your backup connection. Or you can reserve the bandwidth on your main connection for certain types of traffic, and restrict other traffic, e.g., music files, to a maximum of 10% of the available bandwidth. This would also be a precaution against an ISP "denial of service attack" provoked consciously or unconsciously by an employee. You might also consider using a system that would page your IT person if the Internet connection becomes slow or even gets lost.

Environmental Hazards

Imagine you arrive at your office in the morning and the building is closed. Or you are already in your office, an alarm sounds, and you are asked to leave your office immediately. This occurs when a hazardous substance has been detected or if the building is to be closed for police action. In any case, you are standing outside of the building and you do not know when you will be able to reenter your office. And the worst part was that you had no warning that this was coming.

If you think that this scenario is highly unlikely, think again. There are many possible scenarios and many of them have already happened to thousands of small businesses. Whenever air pollutants reach an intolerably high level and government-set limits are exceeded, you may no longer be able to reach your office. Possible causes include nearby accidents, fires with dangerous chemicals and toxic smoke, asbestos fibers

in the air, and foul odors. We also have seen the worst scenario with regard to hazardous material: Chernobyl. The widespread radioactive pollutants will remain in the soil, water, and air of that region for centuries.

For a certain period of time you will need to maintain critical business functions remotely. The environmental hazard may have affected the health of your employees, so you may need to operate with fewer staff.

You can prepare for such an event by having all important documents online for remote access and having your staff appropriately trained and prepared to use a telecommuting infrastructure (which can be convenient even when no disaster has occurred). Of course, there are costs associated with the development of a telecommuting infrastructure, and you need to assess whether the potential benefits justify those costs. You may conclude that the hazardous conditions will likely not last for more than several days, a length of business interruption that many small businesses can tolerate.

Remote Operation: Stage One

In remote operation at stage one, you and your employees cannot physically access your worksite or business office, but the office is still intact and some core systems continue to function properly. You need to prepare in advance so that you can remotely access all important company data and e-mail. The provision for this disaster scenario will have the benefit that it will also allow your employees to telecommute even in nondisaster situations or allow your salespeople to access your company's data when they are traveling. It will permit the sharing of your data with other company offices.

It is a good idea to scan and archive most important documents electronically. You can access them remotely if you are forced to do so under hazardous environmental conditions, and they will be secure. If your building site is compromised in a disaster, you have little control over who will enter your offices and have access to your files. Do you remember seeing television newswoman Diane Sawyer on the air, as she picked up handfuls of documents from businesses in the World Trade Center—documents that had scattered when the towers collapsed? As bizarre as that sounds, here is another example: have you ever attended a ticker-tape parade? I (Stefan) attended a ticker-tape parade when (unshredded)

confidential documents detailing the compensation of senior officers of a particular company landed at my feet. If you need to store original documents, you should store them in a safe that cannot be opened or easily removed. Remember that your business has a legal requirement to maintain certain documents, such as tax records, for a specified period of time. Your legal counsel can advise you as to which documents you must safeguard and over what period of time they must be preserved.

You also want to offer evacuation training to your staff so that they know how to shut down all nonessential office computers, how they can warn all employees using a paging feature on the phone system, and how they may shut down electricity or gas services.

If the hazardous conditions are expected to continue, you may be escorted into your business premises by civil authorities for a brief period to retrieve key items. Therefore, it is a good idea to label all equipment according to your earlier ranking as "critical," "important," or "optional" with large color-coded stickers and larger numbers, so you can, if necessary, ask someone to retrieve item RED#4 for you.

With regard to your phone system, if you used the setup recommended in the last section, turn on your company's cellular phone to continue receiving company phone calls.

You need to agree with your staff on a meeting place where you can convene after your building has been evacuated. If you are a really small company, you can simply meet at someone's home, but if your company has more than 20 employees, you will want to have a separate office site where you can meet. It is unlikely that you will need dedicated recovery sites such as those that large companies have built. It is sufficient if you have a good relationship with a partner company that can give you some temporary place to work, such as their meeting rooms. If you plan in advance, you should make sure that this company is using different third-party providers than your own company so that you are less likely to be negatively affected by the providers having difficulty keeping their operations up and running for other customers not affected by the disaster. And you should have a good stock of spare parts and PCs that are stored off-site and that you can use temporarily.

If you are looking into a secondary site, such as rented office space that you would normally use for client meetings or training seminars but plan to use as a disaster recovery site, review carefully whether that site could function under disastrous conditions. Does it have sufficient electrical power and air conditioning? Is there enough space to store spare

equipment? Your disaster recovery facility requires full third-party services. And of course, your disaster recovery facility's phone, Internet, and utility providers should be as different from your main office as possible. You also need to make sure that you have software licenses for all of your IT systems and determine if any additional computer systems and software licenses have to be acquired.

To reach the main office you need to establish a secure connection, because you will transfer sensitive information, such as human resource records, budgets, and competitive and strategic documents. If you are working at your secondary site, you might consider a dedicated data line back to your main office, if this is cost-effective. Usually, however, you will connect to your office network by direct dial-up or over the Internet using a secured virtual private network (VPN) connection with strong 128-bit encryption. A VPN connection creates a "tunnel" on the Internet through which your data are passed safely; thus, it acts exactly as a private network, and the same security, management, and bandwidth policies can be applied. VPN is a cost-effective network solution that is sufficient in most cases. However, you will want to look into a private leased-line connection between offices if you require a minimum bandwidth guarantee, or if the office locations constantly require exchanging large amounts of data.

There are two solutions for building a VPN network. Software VPN solutions are available and are already part of the Windows 2000 or XP Professional operating systems. A VPN connection can be configured from any client running those operating systems, to a Windows 2000 or XP server machine, independently if they are on the same network or remotely from halfway around the world. The second and preferred solution is built-in VPN functionality in routers. This is especially useful if you like to provide a permanent VPN connection, for example, to connect your main office with your training center offices. If a remote user on the road likes to dial in, he requires additional VPN client software.

System Security

For a small business you want to have at least a classification for document accessibility that translates directly into security measurements on your system. There are at least three categories to consider:

- Public data, for example, brochures, annual reports, and your website. These data are available to all users without special restrictions.
- Restricted access documents, for example, communication with clients or data in your bug-tracking system. This information is generally available internally, but has not been reviewed. It might contain information embarrassing if released to the general public.
- Confidential documents, for example, expense reports, strategy documents, and so forth. These data must be protected because they reveal specific business practices or future plans that should remain confidential.

These three examples represent a basic classification scheme. It is important that security measures are followed to safeguard your business information assets.

In addition to organizing a classification scheme for safeguarding documents, you need to specifically address system security in your business. With a majority of your proprietary information now stored electronically, you are vulnerable to intentional or unintentional misuse by your own employees. Therefore, to integrate these technologies securely and successfully, you must deal with them on an organizational level. The loss or corruption of mission-critical information may have serious financial and legal consequences for your business.

Consider the value of your company's knowledge and information databases. You will need to safeguard this information by an effective and proven security mechanism. These high-security measures are necessary because of the ease with which digital information can be assessed, modified, or deleted, without leaving behind traces of intervention. For this reason, you need to include file access and intrusion detection monitoring with your security efforts. Strong password authentication is also required combined with data encryption whenever data leave the company's network.

Each user account should be protected by a password. Users must choose passwords with a minimum length of eight characters, nondictionary words or names, and a mixed use of upper and lower case and special characters and numbers, like "BGsRGr8t!". Ideally, passwords should be changed every 90 days or so. But from experience in small companies, people don't like to change passwords too often. Sometimes they even share their passwords with colleagues; this practice should be

discouraged. It almost always indicates that the file structure setup is not congruent with the requirements. Did you know that many people use as passwords first or last names of themselves, their children, friends, dogs, or names of cities or landmarks? You would be amazed how quickly hacker programs available on the Internet can decipher such passwords by simply guessing combinations of these items. It hardly takes longer then a couple of minutes to obtain the passwords of at least one-third of average users.

The bottom line is that small businesses do not need complex security measures, but they need *some* measures. Of course, the security measures should be periodically reviewed so that the implemented guidelines meet the requirements and to ensure that they are generally accepted and used. All security safeguards should be periodically assessed and adjusted to meet the latest developments.

Fires and Other Disasters

We now consider disaster types that are destructive to the worksite, be it an office, a manufacturing plant, a retail establishment, or any other type of construction (we will use the generic word *office* to refer to all worksites). Among all of the scenarios, fire is by far the most common hazard that also creates a secondary hazardous condition due to toxic smoke. Natural disasters, like severe weather, earthquakes, and floods, also may damage or destroy your office or at least render the office unusable for some time. In the case of severe weather, however, you often have advance warning of the disaster and can begin an evacuation of people from the premises.

Whatever the cause, you need a disaster recovery site, even if it is only a meeting room at another company's premises. It will take you some time to assess your losses, but you should strive in good faith to provide basic services to your employees and customers and honor your contractual obligations, even though conditions will be challenging. Try to mitigate your losses by maintaining whatever level of operations you can sustain until your business has fully recovered. The effort will be appreciated by your employees and customers.

In addition to assessing which services and products your company is obligated to provide, you should also inquire as to which services and

products you will need from third parties to operate your business in the aftermath of a fire. Determine which other third parties will provide you with temporary services at the disaster recovery site in the event that the permanent provider is also affected by the fire or natural disaster. Identify a priority ranking of which systems must be operational and which data you will need to operate your business even at a minimum level of functioning.

Fire Protection

Plan and discuss with your local fire department the precautions you should take to protect valuable documents or IT equipment from fire. Special fire safes for documents are affordable, and larger safes would also protect against theft and survive substantial mechanical abuse and water damage. You should have an up-to-date, detailed, off-site inventory list of all IT equipment. Labeling your valuable assets with easy-to-read, fire- and water-resistant stickers facilitates subsequent identification and should be used in nondisaster times as an asset control mechanism.

You will find that many traditional businesses, such as law firms, have begun to conduct more and more business electronically. But you will not need all documents online at your alternate site. You need to identify which ones you will need before the disaster strikes. It will be sufficient if you have the documents that you will need for an emergency operation. It is, however, a good idea to plan to store paper copies of all important original documents at a secondary location and determine which documents to make available online.

It is important that you have regular fire drills with the help of your fire department. This should include instructions on how to initiate an emergency shutdown of all systems. It would warn every user that the emergency shutdown is in progress, and that all systems will be automatically shut down in about five minutes. The emergency shutdown can be stopped by anyone, unless it is forced by system administrators. To expedite this process, you can install a “panic” button that would be pushed at the same time as the fire alarm in the event of a fire or an immediate threat, and would shut down all IT equipment within the next few minutes.

Data Backups: Part III

This scenario assumes that the main worksite will be destroyed. Business will continue at an alternate secure location. An emergency replacement IT infrastructure must be ready at that location.

To prepare for this case, if you are using a backup system at your original office location, use a VPN connection to copy all data from your main office location to your alternate office location. Again, a file synchronization tool is easy to use and efficient because it will transfer only the changes that have been made to files during that particular workday. Because the data will be available at the disaster recovery location, a small and simple network can be configured to start disaster recovery operations. You would have the same benefit if you used an online data backup service. In both cases, you will need a fast Internet connection at your disaster recovery site. If you have used traditional methods to back up your data, such as tapes, CDs, or DVDs, you have to retrieve them first from your storage location and then rebuild a file system at the alternate site. Obviously, this is a much more time-consuming task, especially if your data sets are so large that they do not fit the selected medium, and incremental or partial backups have been made and the originals must be restored.

For most small businesses, some form of online storage, like your web server or special online backup space, will suffice. If you have many gigabytes of data that you need during disaster operations, use a file server with large disks at the disaster recovery location. These solutions are more cost-effective and less time-consuming. But there are reasons why you would also want to have backups on removable media, as we shall see in the chapter dealing with sabotage.

If you used a removable backup medium, store it in a safe place that tracks ingoing and outgoing items. Many armored car services offer this service, and they also may pick up and store your backup tapes. Employees should create backups of their own data on the backup system.

The issue is how much downtime your business can afford until you are up and running at your alternate location. If your marketing and sales tools fail, you can probably estimate the direct costs of lost sales opportunities. If your client support tools fail, you have additional intangible costs like blemishes on your public and client relations. And for other systems you will most likely find that variable factors, such as your downtime costs, change over time. For example, if you own a tax accounting

business, you are faced with downtime requirements that change with time. If your system goes down just before the tax reporting deadline, the impact on your business is definitely more severe than a failure later in the calendar year. You can make a rough estimate of the cost of your downtime that should correlate with your disaster recovery budget.

Remote Operation: Stage Two

In stage two, we assume that the computers at your office location no longer function, the communication lines have been cut, and you will not have access to your office premises for some time. The data backup is available at the remote location either from online storage, your own large disk file system, or from removable media. A small office can be built where an emergency operations team handles the most important business functions. You already contracted data lines into that alternate site, and you use cell phones temporarily until you can return to your old site or you have to find a new office altogether.

The question at this point is how to prepare for other services, such as mail delivery. Here, the first step is to establish a secondary location in advance; a virtual office that would handle all your mail even during nondisaster times. If you consider the recent scares about anthrax in letters sent through regular post office mail, you may consider outsourcing mail handling to a third party. As a small business, you cannot afford to buy expensive x-ray machines or to spend the time to investigate each piece of mail. There are various providers of such services. Not only will they accept your mail, but you also can direct them to open your mail, scan it, and send it to you immediately by e-mail. Of course, you also can use them to establish another office presence somewhere else in the world. But the main advantage is that they will receive all mail for you, open it, presort, and forward it to you quickly and efficiently. And if you live in an urban area, it is often possible to receive the most critical mail via messenger on the same business day. Some service bureaus also offer additional add-on services, such as an assumption of payroll and accounting functions. Choose these services based on your budget and your assessment of your likely circumstances should you temporarily lose access to your permanent worksite.

You may consider a bill payment service that will receive your bills for you, scan them, set up money transfers via wire or by check, and let

you decide when and how much you want to pay simply by a preestablished "auto-pay" function or by selecting the bill online. These services are provided by various companies, and are much more advanced than the bill payment services most financial institutions provide with their online systems. We also recommend that you keep a directory of your service providers with your business account numbers, so that in the event of a disaster, you have that information conveniently available to notify your creditors of your circumstances.

Terrorism and Sabotage

Terrorism strikes without warning and is of particular concern as its goal is to inflict maximum damage, including the loss of human life. Deliberately orchestrated violence, such as terrorism, has a profound psychological impact on those who experience it, quite unlike the psychological response to natural disasters. Your first concern is the safety of your employees. There will never be complete protection from terrorist attacks and acts of sabotage. The terrorists will use any mean for their cause, including suicide missions, bombs, and contamination with biological, chemical, or even radioactive agents, if they manage to acquire the material to build such weapons. Terrorists are also becoming increasingly skilled in the use of highly sophisticated IT equipment, trying to "hack" their way into government agencies and into commercial computer systems to steal secret data or to cause considerable damage by altering or deleting data. Because the potential damage is so severe, you need to take protective measures. Similar precautions as for destruction of your office by fire or hazardous substances apply.

Hacker Attacks

As soon as your single home office computer or your small business computer network is continuously connected to an outside network, such as the Internet, some method of protecting your data on the computer or the internal network is required. Any computer system that is directly connected to the Internet will sooner or later be the target of hackers, trying either to penetrate your network, or making it unusable by, for

example, flooding your system with data requests. Also, you have to be aware that the traffic from your network can be watched from the outside as it is often not encrypted. This is even easier when you are connected via a cable modem because everyone on your cable segment can monitor your data traffic.

You need to protect yourself by using firewall software on the standalone PC, or even better, build an internal network and use a network router that separates your internal network from the Internet. There are many router products on the market, and the ones marketed for home office or small businesses often include a firewall where you specify which data traffic you allow through your firewall and which outside parties are allowed access to your network. Usually, you will want to allow all traffic that was initiated from inside your network to pass the firewall from the outside. Traffic initiated from the outside should only pass the firewall if it is in response to a former request from the inside, or if you have specific machines and applications that you would allow access into your network. But for the general public you would either refuse the data packages or route this traffic to a separate network called the demilitarized zone (DMZ). Here you would place, for example, a testing web server, or a place where you make the latest information available for salespeople connected to the Internet.

Although this might appear complex, the configuration of these routers for home offices and small businesses has become fairly simple. Most routers now provide web-based interfaces with good online help. But that alone is not a guarantee that it will be simple. Some products come with web interfaces that are poorly designed, or require firmware upgrades before they can work with your ISP.

The advantage of a network router is that the connection to the Internet is simplified because all ISP-related network information is configured only once in the router, and communicated to all internal machines automatically if the standard protocol is supported.

However, if your ISP is charging you based on the number of computers you have connected to the network, and you use a router, you have only one connection point to the ISP's network. The ISP can detect a router from its hardware Ethernet address. Most off-the-shelf routers have a built-in function that allows spoofing the address of the router by substituting an address from an internal computer, so the router will appear as a computer from your internal network. Check with your ISP first.

We do not recommend using a computer to act as a firewall or a router or both. Stand-alone network components are much easier to set up, are inexpensive, and provide a much higher guarantee that you have not created any kind of loophole in your setup that would compromise network security.

A firewall is only one step in a larger network security scheme that must include a security policy, automatic intrusion detection, and monitoring for viruses that can sneak in with regular traffic. There are also various solutions that you can run on a PC that will allow the PC to be accessed from the outside, even if a firewall is in place. These software packages mimic the same traffic as web browsing would, but instead of website information, they send data about your PC and the files on it. With some software packages you can remotely take control of your PC, although your firewall does not allow any traffic initiated from the outside. This is possible because in this case the traffic is initiated from a small application running on your PC, and therefore for the firewall the traffic appears to be legitimate because it was initiated internally. You can use it to your advantage, but you also need to be aware that certain security risks accompany it.

Make certain that virus protection is current to avoid compromising your security by viruses and Trojan horses entering your system. You also need to regularly update your operating system. Updates are provided nearly every week. It is important that you train your users how to handle suspicious e-mail attachments and how to detect virus-like activities. Your ISP or e-mail provider can often provide additional security measures.

Be aware that even cell phones can become the target of virus activities, particularly if they are in the league of the new Internet-savvy phones that allow you to browse the Internet. We expect that such devices will be standard in a couple of years, and then they will behave like any other computer on the Internet.

Your overall attention to security issues and the technical expertise that you obtain will determine the effectiveness of your security precautions. Do you always remember to remove accounts for employees who have left the company? Special care should be taken if a system administrator leaves because he usually knows back doors into your systems.

Internal Sabotage

A good system administrator builds his or her reputation on the trust that he has earned throughout his career. But even with the best system administrator in the service of your small business, you are obligated to protect your company against attacks by internal sabotage. These measures are not too difficult to implement and should be welcomed by your systems administrator as being in the best interest of the company. There are some basic auditing methods that you can apply and review periodically, such as identifying who accessed which files, who generated which external network traffic and who sent a large number of e-mails or large attachments to which addressee. You should, of course, inform your staff that you are monitoring activities on the company's network, and the results of these activities are not matched with personal information unless there is a compelling reason to do so. Staff should also refrain from storing personal information on company computers. These guidelines should be formalized in company policy.

Although it is practical to make backups from one disk to another disk, it is also important to occasionally make a backup on a removable medium and to store this backup in a bank safe that is not accessible by the system administrator. The system administrator probably would also want a bank safe to store his backups, but he should have a separate one, preferably at a different bank.

Having outsourced your e-mail to a third-party provider, you already took an important step to be independent of internal systems staff for your e-mail service, thereby reducing both the work burden on the staff and the opportunities for internal sabotage.

Insist that the passwords for all equipment, particularly for network equipment, are given to you in a closed envelope. You want to keep it closed, unless there is a major emergency or your system administrator leaves the company. Then it is best to have another system administrator come in to change the entire list of passwords. In fact, we suggest that you do not use any built-in "administrator" accounts, but instead, give two user accounts administrative rights on the system. This way each week those two people can independently monitor and audit suspicious activities on your network, and system administrator tasks can be traced to their user identifications.

Even so, your business could be the target of a saboteur who "infects" your network with a virus. Usually with good protection in place, this should not be an issue, but we often see that in small businesses passwords are not safeguarded, users' permissions are not set, everyone can have system administrative access, and files are open for everyone to read and for everyone to delete. You have to be aware of this and take the necessary precautions. Review your protection scheme regularly.

FINANCIAL LIQUIDITY

Thus far, we have presented information to enable you to prepare for a disaster and to develop a contingency plan with respect to the information technology infrastructure of your small business. We have placed a special emphasis on developing redundant capacity; that is, having additional sources of computing power and backups of all data and records for your small business readily available in the event of a disaster. We now apply the same concept to the financial elements of your contingency plan, in effect, developing redundant financial capacity, by means of various tools, such as insurance. If a disaster should strike your business, you may need additional funds to replace lost or damaged assets and to cover additional operating expenses during the recovery period following the disaster. Let's begin by examining the role insurance plays in contingency planning.

Role of Insurance

When you made the decision to start (or to join) a small business, you assumed certain risks. You almost certainly did so because you believed that the rewards you would receive were commensurate with, or disproportionately generous to, the risks you would assume. These rewards may include the freedom to chart your own course, the ability to own your own life and to balance work and family, the joy of realizing a creative vision, and the financial rewards that come with entrepreneurship. You almost certainly took steps to mitigate your risks. Entrepreneurs are, by nature, resilient and resourceful. We are optimists, and believe we can create a better future for ourselves. We are also reluctant to jeopardize our small business vision, our future, by taking needless or reckless risks.

All successful entrepreneurs take prudent risks, most likely beginning with the formation of your company!

When you started your business, your legal counsel almost certainly advised you about the need to incorporate in order to minimize your personal liability, among other reasons. Your insurance program is the next step in the process of mitigating risks to enable your small business to succeed. A carefully crafted insurance program protects your business assets against the risk of *unanticipated* losses, italicized for emphasis. We would advise you not to insure against *anticipated* losses, as it usually is not cost-effective to do so. Consider the example of extended warranty programs for office equipment, which are analogous to insurance on single pieces of equipment. We decline to purchase such coverage, because we expect that office equipment depreciates and must be replaced from time to time. As such, we can budget for it. I (Donna) chose not to pay $150 for an extended three-year warranty for the $600 multifunction laser printer/digital copier that sits in my office. The printer has functioned adequately for the four years that I have owned it. It shows the signs of normal wear and tear and I will likely replace the printer within the year. Newer models with features comparable to my existing printer can be purchased for $450. Clearly, the extended warranty plan (which covered anticipated costs to repair the equipment due to normal wear and tear) would not have been a sensible investment.

I did, however, have my printers covered under a business owner's policy. When an unexpected disaster occurred, the insurance benefit mitigated my loss. Our business insurance policy provided for each of the printers and fax machines which were damaged by ash and soot from the collapse of the World Trade Center towers to be removed from the office and professionally cleaned and serviced. In some cases, drums and cartridges were replaced. The insurance policy paid for the repair of those machines that were damaged as a consequence of an *unanticipated* event—certainly no one expected a disaster of the nature that occurred on September 11. Those losses were not inconsequential; the cost to repair a single printer or fax machine was $250. The insurance premium I paid for this benefit was a sensible investment for my business.

This is the first take-home lesson of crafting your insurance program: it is generally not cost-effective to insure against anticipated losses. Consider which losses you can predict and for which you can budget. Those losses can be self-insured, or paid for out of your cash and short-term cash equivalents account. The extension of this lesson is the insurance deduct-

ible. The deductible is the amount of losses that your business must bear before your insurance policy pays a benefit. Generally, the higher the deductible (or the greater the amount of losses that you will bear before your insurance policy is obligated to pay a claim), the lower the premium. Discuss with your insurance agent the options available to you so that you may select the deductible that is appropriate for your business.

You likely see how this lesson applies to your personal insurance program. It bears repeating: generally it is not cost-effective to insure against anticipated losses. We see many small business owners who pay premiums to cover losses that they could afford to bear themselves, but they fail to insure against risks that would be catastrophic if they occurred. The same is true of individual policyholders who often don't transfer risks to the insurance markets in a cost-effective manner. For example, consumer advocates report that many credit life insurance programs (insurance that pays the installment debts of the insured at his death) are not cost-effective. They argue that consumers would be better served by purchasing other forms of life insurance for which the cash benefit would be available for a broader range of uses. Those very same consumers may be uninsured for other types of risks that could be covered by a broader life insurance policy. Spend your insurance premium dollars wisely: purchase coverage for unanticipated losses, not expected and predictable ones.

Now that we have persuaded you (we hope!) that your insurance program should be crafted to cover unanticipated losses, let us consider some of the risks you should insure. Many insurance companies bundle property and liability coverage into a product known as a "business owner's policy," or sometimes it is referred to as a "package policy." It allows the business owner to obtain broad coverage with affordable premiums. Since each business is unique (and each business owner's level of risk tolerance is unique), insurance coverage can be customized to suit the particular needs of the business. A retail sales operation has different insurance needs than a restaurant or a dentist's office. Because we cannot reasonably anticipate the individual circumstances of each of our readers, we endeavor in this chapter to give you the tools you need to enter into an informed discussion with your insurance broker.

Your insurance broker may begin a meeting with you by discussing monoline policies, or policies that cover against the risk of a single peril, such as fire or auto theft. Business owners' policies and package (or multiline) policies are the sum of two or more monoline covers, except that the premiums for the whole package policy are generally less than the sum of the parts of constituent monoline policies under a property-casualty insurance program.

It will be helpful to prepare an inventory of business assets to be insured prior to meeting with a broker to discuss the program for your business. Many software packages for small businesses provide for an inventory of property, plant, and equipment. You can record the date of purchase, the model number of the equipment, the manufacturer's name, and the purchase price. Many of these programs interface with your accounting ledgers to update your depreciation expense as appropriate. You may also take digital photographs of key equipment, such as office furniture and other items to keep with your records, item by item. Obviously such records are helpful in documenting losses should a disaster damage the assets of your business.

But these records are also helpful in assessing the amount of property you need to insure. You may be surprised when you calculate the replacement cost of all of your business assets and will be relieved to have that figure available when selecting the appropriate insurance coverage for your business. We suspect that many small businesses are underinsured for property losses because the business owners underestimate the value of their assets. When you include everything that would have to be replaced in the event of a fire or similar catastrophe, it adds up. It bears repeating: make multiple copies of these records and store one or more off-site. Your receipts and photographs of business property are of little use if they are destroyed in a disaster.

Property-Casualty Insurance

Property insurance protects the assets of your business against losses arising from perils such as fire and theft. Basic form commercial prop-

erty coverage typically protects your small business against the following perils:

1. Fire, plus extended coverage, such as:
2. Lightning
3. Explosion
4. Windstorm/hail
5. Smoke
6. Aircraft or vehicles
7. Riot or civil commotion
8. Vandalism
9. Sprinkler leakage
10. Sinkhole collapse
11. Volcanic activity

Broad form commercial coverage includes basic coverage for fire (peril #1) and extended coverage (perils 2–11), in addition to:

12. Breakage of glass
13. Falling objects
14. Weight of snow, ice, or sleet
15. Water damage

Special form coverage provides so-called all risk protection. The term *all-risk* is misleading, because it doesn't necessarily cover all risks, it typically covers basic form risks, broad form coverage (perils 1–15), and other causes of loss, such as earthquakes, unless the peril is specifically excluded from coverage. Read your insurance policy carefully to understand which perils are excluded from coverage. Property coverage options may include endorsements, or additional risks covered. Table 1.1 lists some of the endorsements that may be available for coverage under your insurance policy.

This table does not present an exhaustive list of perils for which endorsements may be obtained, but it is sufficient to start you thinking about the types of risks you should discuss with your insurance broker. The design of your insurance program will be highly customized to suit the unique needs of your small business. For example, like many small business owners, I (Donna) maintain a refrigerator in my office stocked with fruits and other perishable foods for consumption by employees and

Table 1.1 Possible Endorsements to Property-Casualty Policies

Accounts receivable	Additional insured endorsement	Automatic annual increase in building limit of insurance	Automatic annual increases in business personal property	Boiler and machinery
Civil authority	Consequential loss	Crime	Data processing, and hacker's insurance	Debris removal
Earthquake	Electronic media and records	Fine arts	Fire protective equipment discharge	Improvements to the property
Increased cost of construction	Inland marine	Intangible property, such as trademarks	Loss of rents	Mechanical breakdown
Mobile property	Personal property of your employees and/or customers	Personal property off premises	Property of others under your care, custody, and control	Refrigerated food spoilage coverage
Signage and other outdoor property	Trees, shrubs, and other landscaping	Transportation	Utility services	Valuable papers and records—cost of research

visitors to the office. When our office building lost electricity, the food was spoiled and we had to throw it out. We were not reimbursed for this loss, as I believed that it was a loss we could afford to bear and so did not seek to include such an endorsement in our insurance policy. However, if my small business were a restaurant, it would be an altogether different matter. Imagine if the supply of electricity to a restaurant were disrupted. The business could easily lose $50,000 or more due to spoilage of meats and fish. For a food-service business, a policy endorsement for refrigerated food spoilage coverage may be critical.

To ensure a prompt and fair settlement at the time of loss, your insurance policy will likely specify the valuation method used to determine the value of your assets covered under the policy. Your policy may provide for replacement cost, or the actual cost of replacing an asset, with-

out deducting depreciation. It may provide for an actual cash valuation, that is, the replacement cost of the asset less the accumulated depreciation. Finally, the policy may specify that the valuation method is an agreed amount or functional replacement cost. This is the method most commonly used for works of art and other unique items for which it can be difficult to obtain an objective valuation.

By the way, items such as plants and fish in the office aquarium are generally not insurable, but the aquarium itself and its equipment are insurable. Property insurers won't underwrite the cost of replacing living organisms, such as plants and fish. They consider aquarium fish to be pets. But the aquarium, filter, plant pots, and so forth are property that can be insured. I (Donna) share this with you because I have a soothing 25-gallon aquarium in my office. The maintenance person who comes periodically to service the tank related an anecdote of another of his clients who had a large salt-water aquarium gracing the reception area of his small business, a commercial real estate brokerage. Because he considered it a decorative item, he had not thought to obtain insurance for it. It was damaged in a disaster and the cost of replacing it was $50,000. He could have insured it for several hundred dollars. Photographs and receipts can be helpful in documenting the loss, because obviously there is no standard replacement cost for such items—an aquarium can be a modest desktop unit with 10 gallons and a few goldfish, or it can be a custom-built floor-to-ceiling decorative piece with exotic fish, as this gentleman apparently had in his office. Receipts and photographs will help you to come up with a fair assessment of the replacement cost.

We generally recommend electing to value assets on the basis of replacement cost. It facilitates settlement of your insurance claim by avoiding a discussion of accumulated depreciation on each damaged asset. It also provides you with the funds you need to replace damaged assets immediately. We are particularly sensitive to insuring IT equipment. The PC you bought five years ago may no longer be available, and you and your insurance company will have to identify a model available on the market with comparable features to your old PC in order to establish a fair replacement cost. We recommend keeping records of the functional specifications of your IT equipment for that reason. If you know the memory, disk size, and other functional specs of your machine, you can easily identify a com-

parable model. If you record that information now, it will save you time and aggravation should disaster strike later. In disaster-recovery mode, you don't want to waste time searching through old sales literature to determine the processing speed of your damaged computer for the purposes of identifying a comparable model.

Before we conclude our discussion of property insurance, we would like to call your attention to a specific insurance policy endorsement that is rarely considered by small businesses: disruption of electrical supply. We know of many small business owners in Lower Manhattan who elected to forego coverage for this peril, believing that the surge protector equipment that they had in place was adequate to protect their computer equipment from anticipated fluctuations in electricity supply delivered to their offices. The attack on the World Trade Center changed those assumptions. Much of Lower Manhattan was left in the dark for days following the disaster, and businesses cannot operate in the dark. Consider carefully whether you wish to purchase coverage of additional perils, and if so, at what cost.

This section of the chapter is titled "Property-Casualty Insurance"; "casualty insurance" is insurance-speak for liability insurance. Liability insurance protects the assets of your business in the event that you or one of your employees is accused of an act that causes injury or damage to another person or property, or that such injury or damage is the result of your failure or the failure of one of your employees to take action to prevent such injury (also known as negligence). Liability insurance typically covers not only the costs of the damages, but also the legal and other expenses associated with resolving the issue of liability. In the context of this discussion, remember that we are considering liability insurance with respect to contingency planning for a disaster—an event that disrupts operations at one or more of your business sites. The needs of your small business for liability insurance (and property insurance) are much broader than what we are presenting in this book. For example, we would recommend that your business carry employment practices liability insurance to protect your business against claims of sexual harassment, wrongful termination, or other types of employment-related lawsuits. However, this need is unrelated to contingency planning, based on the definition of disaster we set forth in the Preface. Similarly, professional liability insurance is a coverage we would recommend for professionals

such as physicians, dentists, architects, engineers, or attorneys to protect them against liability for negligence or malpractice. However, this is a topic for a general primer on business insurance, not for contingency planning and disaster recovery.

Liability insurance policies might include endorsements for personal injury (arising from claims made for libel, slander, and so forth), host liquor liability, fiduciary liability, or fire legal liability. With respect to disaster planning, there is a risk that your business could be held liable for injury or damages should you have inadequate contingency plans in place. For example, imagine that a fire occurs on your premises. The main entrance to the office is burning and so you must seek an alternate means of egress. The only other exit from your office is by means of a back door that has been boarded up and is blocked by storage boxes and crates that cannot be removed in a timely manner. Your business could be held liable for the loss of life that could have been prevented had there been a second, safe, means of exiting your business premises.

There are certain types of liability coverage that we would encourage you to discuss with your insurance broker as you design your insurance program and your overall contingency plan. The first is business interruption insurance, a form of insurance that pays a benefit to your small business following a disaster when your business is unable to resume operations. Because this form of coverage is so important to your contingency plan, we devote a separate section of this chapter entirely to business interruption insurance. Next, we want to call your attention to commercial auto insurance. Certainly we expect that your small business has its vehicles insured for physical damage and liability. But what you may not have appreciated is that you also may require insurance, known as "non-owned automobile coverage," if you or your employees use personal vehicles when on company business. Imagine that one of your employees offers to drop a package off to the office of your client, because the office is located on her route home. If she is in an auto accident during the course of that trip, your business could be sued for damages even though your company does not own the employee's car. Consider carefully whether you should include non-owned automobile coverage in your overall insurance program. Such a policy also may

cover rental cars when you travel on business. Hired and non-owned automobile coverage is relatively inexpensive and, in our opinion, an important part of your insurance program. Should a disaster require you to operate from an alternate location, you may be renting cars and commingling personal commutes with business tasks; non-owned auto coverage will protect your business against the additional risks assumed.

When thinking of operating your business from an alternate location, consider insurance coverage for your home office. If you work from home, either in the normal course of affairs or in response to a disaster limiting access to your customary business premises, you should update your homeowner's policy to include coverage for the office equipment in your home and business liability coverage for the business activities you conduct in your home. This coverage is not automatically included in a standard homeowner's policy. If you rent your home, you may want to include your home office equipment in your tenant's insurance policy. If your business has issued equipment to employees for use at home, such as laptop computers or mobile telephones, be certain that those assets are insured through your commercial policy. It is an easy mistake to omit assets from your inventory of property, plant, and equipment when they are off the premises.

Next, workers' compensation and disability benefits insurance are typically mandatory coverages for businesses, depending on your state's requirements. Should a disaster cause injury to an employee on the job, these components of your insurance program will be very important to the recovery of your employee and your business. Workers' compensation insurance protects employees against the risk of sustaining a job-related injury. Workers' compensation insurance covers medical expenses, disability income benefits, and death benefits to dependents of an employee whose death is related to his job. Premiums are assessed according to payroll and depend on the industry classification of your business. An advertising firm would pay lower workers' compensation premiums than those paid by a construction company, reflecting the relative risks of injury to employees of those two businesses. That is why

it is important that you classify employees accurately for their job descriptions and wages. If you are adding new employees to your payroll, be certain to update your workers' compensation coverage to avoid incurring an audited additional year-end charge.

Obviously, the risk of incurring workers' compensation–related claims increases with the occurrence of a disaster: employees may injure themselves while evacuating the business premises, and stress-related injuries, depression, and other types of disorders may occur as a result. Be certain that your workers' compensation coverage is up-to-date. Similarly, employees injured in disasters while on the job may require disability benefits. Certain states mandate coverage for short-term disability for all employees. Check the website of your state's insurance commissioner or consult with your insurance broker to learn the requirements of your state.

We have three suggestions that may help to reduce your workers' compensation premiums (and possibly enable you to pay for non-owned automobile coverage or other insurance coverages that your business may need). First, ask your insurance company about merit-rating credits. In most states, small businesses that have favorable claims experiences may be entitled to credits toward their premiums. Second, consider adding a deductible to your workers' compensation policy. Workers' compensation typically covers from the first dollar of losses, but most of the states allow deductibles, which will reduce your costs. Finally, consider foregoing coverage for yourself or for other officers or directors of the company. Many states let small business owners and certain officers and directors opt out of their workers' compensation policy. This would lower costs, but you would be left without workers' compensation benefits should you be injured on the job. This may make sense if you have medical insurance to pay for medical expenses incurred in an on-the-job injury or other means of financial support, such as a disability income policy, if you or any of your directors and officers were medically unable to work.

Director's and officer's liability insurance (commonly known as D&O) is an executive protection policy that covers directors and officers who may become personally liable for their actions on behalf of the company. With respect to contingency planning and disaster recovery, any corporate action that may have increased the company's loss may give rise to a D&O claim. An employee injury on the job or a fire at the company plant, for example, may result in a suit against the officers and directors of the company for their alleged failure to take steps on behalf

of the company to mitigate the risk of fire, such as installing smoke detectors or training employees in basic safety practices.

Stefan worked at a site in which regularly scheduled fire drills would provoke concern from the firemen when the doors to the exit stairways were found to be locked, thereby blocking a safe evacuation by that route. Should a fire occur, the insurance company may deny parts of the claims for damages, on the grounds that the building management failed to mitigate potential losses by ensuring that the exits were not locked.

It is important to involve all of your directors and officers in developing contingency plans for the business and to ensure that the directors and officers are adequately protected against the liabilities that may be incurred in serving the company. Your contingency and disaster recovery plans may one day be reviewed and, with 20-20 hindsight, found to be insufficient by some measure. Limit your liability with the purchase of D&O insurance.

Indeed, the need for insurance expertise may be a consideration when assembling your company's board of directors or advisors. I (Donna) was asked to serve on the advisory board of a high-tech, start-up company, in part because of the company's interest in my reinsurance experience. Each of the members of the board of advisors was recruited because he or she possessed some specific expertise, be it marketing, public relations, or regulatory experience, that augmented the talent available to the management team of this particular company. The advisors were compensated with stock options, thereby conserving the cash of the start-up operation. You might consider a similar arrangement for your company.

Along with D&O coverage, we encourage you to consider a "key person" insurance policy. If you or any other individual are so critical to the operation of your business that it could not continue in the same manner without you, you should consider "key person" insurance to finance the continuity of operations during a period of transition caused by the death or disability of an owner or "key employee" of your small business. This type of insurance policy is frequently required by government loan programs, venture capitalists, and banks. If the financial performance of the business is dependent on a key employee, the bank or other lender will want some type of protection should the key person become incapacitated.

In addition to key person and D&O coverage, consider purchasing excess liability coverage, also known as an "umbrella" policy. This type of policy provides benefits when the limits of the basic, underlying policy are exhausted. Umbrella coverage allows you to substantially increase your insured coverage for a relatively modest incremental cost. The amount of coverage your business needs depends on the size of the business and what we call the "p-o-m" factor—what you require to have peace of mind.

In determining your insurance needs for contingency planning, take into consideration other requirements of your business to ensure that you do not omit or duplicate required coverage. For example, if you rent your office facility, your lease likely specifies that you are required to maintain insurance on the space you lease and to name your landlord as a beneficiary. In the event an employee or visitor to the office causes damage to the property, the landlord wants to be certain that you can reimburse that loss. Your type of business may require specific insurance coverage, such as surety, to provide a guarantee to your customers. Look at your insurance program in total, not in a piecemeal fashion, to ensure that your business is adequately covered.

Business interruption, workers' compensation, key person, disability benefits, D&O liability, non-owned automobile liability, and home office insurance are some of the types of coverage you should consider including in your insurance program as part of your overall contingency plan. As we stated at the beginning of this section, business owner policies often offer a relative bargain, bundling different types of insurance covers for a single premium that may be less expensive than the costs of purchasing each additional cover in a separate monoline policy. We have one final suggestion before we conclude this section: industry-specific covers. Many insurance companies have developed insurance programs specific to certain industries. A visit to the website of a property-casualty insurer, for example, may list a menu of options of coverage for businesses in the financial services industry, or businesses in a certain profession, such as dentistry. These insurance programs include specialty coverage that is advantageous to the businesses in those designated industries and may give you free or low-cost access to consultants who can advise you on how to reduce your risk of loss. In our experience, these specialized industry covers are well worth the premium. They also may include business interruption protection customized for the unique needs of your business.

Business Interruption Insurance

A disaster, such as a fire or flood, may interrupt your business. Until your business recovers from the disaster, it may experience a loss of income, while at the same time being responsible for fixed obligations such as rents and payroll. Property insurance may pay the cost of replacing assets damaged by the fire or flood, but your business may have difficulty meeting its obligations until the damaged assets are replaced and the business is once again fully operational. Business interruption insurance is designed to mitigate that loss.

Let us consider an example. We know a dentist whose premises were damaged in a storm that shattered the windows and left debris and broken glass throughout the office. Property insurance covered the costs of replacing the broken windows and removing the debris and broken glass from the dentist's office. Three weeks were required to assess the damage and to make the necessary repairs, during which time the dentist was unable to see patients in his office. He was liable for his office rent, payroll, leased equipment, and other ordinary business expenses during that time, but he received no revenues. If he had been covered with business interruption insurance, he could have demonstrated what his average daily revenues had been prior to the disaster, and sought reimbursement of that sum per day for the number of days that his office remained closed for disaster repair.

Business interruption insurance was generally not well-known within the small business community until Hurricane Floyd struck in the United States and the recent storms in Europe resulted in longer-than-expected recovery times for small businesses to resume operations. Frequently, it was the loss of income, rather than the loss of property (which was often insured), that caused small businesses to file for bankruptcy protection. We have found many small business owners in Lower Manhattan who did not have business interruption insurance, because they were not aware of it. Imagine if your restaurant or your printing press or your barber shop is closed by civil authority for several weeks. Could you afford to forego that income, given that you still have obligations to meet?

Business interruption insurance is typically sold as an endorsement to property insurance policies. It indemnifies policyholders for losses associated with insured interruptions of their businesses. In effect, it is designed to pay your business what the business would have earned had a disaster not disrupted the business operations. Because business inter-

ruption insurance is an endorsement to a property insurance policy, it cannot be purchased separately. That is, your business must first sustain an insured property loss before the business interruption coverage is "triggered."

Let's consider a real-world example. A husband and wife own a sandwich shop and close the business for three weeks when the husband is hospitalized for major surgery and the wife remains home to care for him during his period of recuperation. During this three-week period, no income is earned as the shop remains closed. Can they claim a benefit under their business interruption coverage? The answer is no, because their business did not sustain an insured property loss. The husband's absence from work was independent of the conditions of his business.

Many small businesses will derive limited benefit from certain of the disaster recovery recommendations in this book, owing to the fact that their businesses are immobile. For those businesses, the business interruption coverage is particularly important. Consider a restaurant, for example. As a restaurant owner, you can (and should) back up your data, such as tax records, employee wage records, customer accounts, and other information. The IT contingency plan recommended in this book will prepare you for the first three (and the most common) disaster types: human errors, equipment failures, and service failures. But an event that displaces you from the worksite (caused by environmental hazards, fires and other disasters, or terrorism and sabotage) leaves you with few options. You cannot operate a restaurant or a retail store from a remote location, even on a temporary basis. The business interruption is particularly important to cover the lost revenues for businesses that cannot relocate.

We have interviewed small business owners in Lower Manhattan and in Florida who were affected by separate, unrelated disasters, and our findings were the same: small business owners were frequently not aware of the possibility of business interruption insurance. Because the endorsement is an incremental expense to your property coverage, we strongly recommend it. Should your business sustain such a loss, you must be prepared to present a reasonable case for "pro forma" business income; that is, what you would have earned during the period of time that your business had not yet resumed operations. The accountants for your insurance company will request documentation of your fixed expenses, such as your office lease and payroll records. They will also request documentation of prior income, such as business contracts and prior period

tax returns. To the extent that you can produce this information quickly, you can expedite processing of your claim—another reason why you should prepare for a disaster and keep a second set of business records off-site where you can retrieve them should a disaster strike your primary worksite.

Selecting an Insurer

Designing an insurance program suitable for the unique needs and limited resources of your small business is an important project. There are three types of insurance professionals who can advise you with respect to your insurance program:

- Agents are licensed representatives of insurance companies responsible for marketing their products. They typically earn commissions based on sales volume. An agent may represent only a single company (a captive agent) or several companies (an independent agent).
- Brokers are licensed representatives who work with more than one insurance company, but represent the interests of the buyer of insurance and recommend the insurance program in the best interests of the buyer. Like agents, brokers earn commissions based on sales.
- Consultants may help to assess the needs of the business, design an appropriate insurance program, and recommend a suitable insurance company. The consultant is paid a fee for his service by the business. For large global corporations, consultants may earn their fees by offering specialized expertise with respect to insurance requirements in different locales; therefore, their fees may be considered a wise investment. For small businesses, however, agents and brokers can generally provide the same advice without incurring fee obligations to consultants.

We would like to suggest that you consider another resource that is free to small businesses: SCORE (Service Corps of Retired Executives). SCORE is a program of the Small Business Administration that is staffed by volunteers, retired executives who seek to share their experience and guidance to help small businesses grow and prosper. To find the location

of the SCORE office nearest you, visit *www.sba.gov*. Your local SCORE office will match you with a SCORE volunteer whose experience is appropriate for your needs. We know of several savvy small business owners who sought to be matched with SCORE volunteers who were retired insurance executives and so benefited from their experience at no cost.

Once you have selected an advisor to guide you through the process of developing an insurance program, you will need to select an insurance company carrier. As small business owners, we must husband our resources carefully, but we urge you not to select your insurance carrier solely on the basis of premium. Cost should be only one of several criteria that influence your purchase decision. Claims-paying ability, or the financial strength, of the insurance carrier is another of the criteria you must consider. Rating agencies, such as Standard & Poor's and A.M. Best, assess the financial strength of insurance companies based on the quality of their balance sheets, their financial reserves, and other criteria that determine their ability to pay policyholders' claims. A strong claims-paying rating is evidence of financial strength and the insurer's ability to pay policyholder claims. A weak claims-paying rating may be cause for concern; as a small business owner you would not wish to pay premiums to an insurance company only to see that the insurance company becomes insolvent and is unable to pay your claim.

You may obtain the financial rating of the insurance company from the agent, the broker, or the company itself. You also may go to your public library and read the reports from A.M. Best or Standard & Poor's to learn more about the financial strength of the insurance carriers you are considering. You should also do some research about the insurance company's quality of service and record in the small business market. Consult with other small business owners to learn of their level of satisfaction with their insurance carriers. Your state's department of insurance, which licenses insurance companies to operate within the state's borders, is also a good source of information about insurance companies and consumer complaints.

We encourage you to consider working with an insurance company partner of an association that represents the interests of small business owners. As an association member you are likely to have some assurance of superior service from the insurer than you would have as a single insured entity. We can suggest a few associations for you to look into, such as NAWBO (National Association of Women Business Owners) and NFIB (National Federation of Independent Business). Dues-paying members

of NAWBO have access to a range of resources that may be helpful in contingency planning and disaster recovery. The NAWBO speaker's bureau, for example, may help you to identify fellow members with expertise in insurance and risk management with whom you can network. Fellow members can share with you their experiences with their insurance carriers and make recommendations. Finally, corporate partners of NAWBO include insurance companies that are eager to serve NAWBO members and offer specialized services.

NFIB represents the interests of its member small businesses. NFIB also offers its members discounted property-liability insurance programs. NFIB's publication, *Smart Business,* frequently covers insurance and risk management topics and presents case studies of its member businesses that are very helpful. I (Donna) am a member of both organizations and I find that the benefits to my business far exceed what I pay in membership dues, including high-quality service from outstanding insurance carriers affiliated with these associations.

Some small businesses will find that they are not insurable as risks in the "standard" marketplace and may have to turn to special insurance facilities that serve the residual, or nonstandard, market. These special facilities include the excess and surplus lines market, the national flood insurance program, and the state insurance underwriting associations.

The excess and surplus lines market consists of insurance companies that underwrite special risks. These companies are often nonadmitted carriers; that is, they are not licensed by the state insurance departments, so care must be exercised in purchasing such coverage. An ordinary commercial insurance broker can refer you to an excess and surplus lines broker, if he or she is unable to obtain coverage for your risks in the standard market. One engineering firm with which we spoke obtained its excess liability coverage in the excess and surplus lines market when it was unable to obtain coverage in the standard market. Because such coverage is relatively expensive, your broker should make every effort to place your insurance program in the standard market.

The standard market will typically not provide flood insurance in monoline or business owner's policies. You may be able to purchase insurance coverage against losses arising from floods through the National

Flood Insurance Program if your business property is in a community designated as a special flood hazard area and if that community enforces measures designed to reduce future flood risks. This program is administered by the government's Federal Emergency Management Agency, and you may obtain further information from their website, *www.fema.gov*.

Finally, states sponsor pools of insurance companies that underwrite nonstandard risks to businesses operating within the state borders. For example, the New York Property Insurance Underwriting Association is a pool of insurance companies that underwrite fire insurance in New York State. The Association offers fire and extended coverage as well as coverage for vandalism and sprinkler leakage to small businesses that are unable to purchase this type of insurance from commercial insurers. The Association also provides business interruption insurance to companies based in New York. However, the Association assesses premiums that are substantially higher than premiums assessed in the standard market. Special insurance facilities in each of the states offer coverage to those unable to obtain coverage in the standard market; for further information, visit the website of your state insurance commissioner. However, premiums in the nonstandard market are generally more expensive than premiums in the standard market, so you should adopt risk management practices to facilitate the placement of your risks in the standard market.

Risk Management

Risk management is a set of practices that will enable you to identify and minimize the risks that your small business assumes. Generally, a risk management program consists of four sets of practices:

1. **Risk avoidance practices.** Your small business should avoid risky activities whenever possible. We expect that many readers will chuckle upon reading this, as you say "Of course, no sensible business owner would undertake risk unless it was necessary to the business operations and commensurate with reward" and you may wonder why we are stating the obvious. Yet, we are amazed when we read of businesses that sponsor company outings at which employees burn the soles of their feet walking across hot coals in an effort to build camaraderie. Isn't that a risk the business could painlessly shed? What arrangements do you make for

liquor service at the annual company holiday party? Do you arrange transportation home for those who consume alcohol to avoid the risk of a tragic accident? Consider risks that you can remove from your business without diminishing your business operations.

2. **Risk reduction practices.** Seek to reduce the risks you cannot avoid. For example, you might install a security camera in your retail store to reduce theft. You might place smoke alarms throughout your office to detect smoke and fire. You might provide your workers with specialized equipment to reduce the risk of workplace injury. You might adopt a policy of not allowing key officers of the company to travel together on the same airline flights.
3. **Risk retention practices.** You will retain some risks and insure others. You may choose to increase the risks you retain by raising the deductible. Higher insurance deductibles generally mean lower insurance premiums. Higher insurance deductibles generally also reduce the frequency and likelihood that your business will file claims, and a favorable claims experience also reduces premiums. Be certain that you have set aside sufficient cash in a reserve fund to pay the losses until the deductible is reached and to cover your essential business expenses until at least part of your insurance claim is paid.
4. **Risk transfer practices.** Some of your risks may be transferred by insurance, some may be transferred by other means. For example, if you provide advisory or consulting services, you may require your clients to sign an indemnification agreement, in which they hold you harmless from liability for the advice you provide.

A sensible risk management program, one that reduces your risks, may make your business more desirable to insurance companies in the standard market and reduce the risk that you will have to pay more expensive premiums in the nonstandard market. We conducted an informal survey of twenty commercial insurance brokers and asked if they could identify the mistakes most commonly made in risk management and insurance programs by small businesses. Here are the three most commonly cited mistakes cited in our unscientific survey:

1. Failure to obtain adequate insurance on vehicles used for business purposes.
2. Failure to cover family members who work for the business under workers' compensation and disability insurance programs.
3. Failure to review the insurance program on a regular basis to ensure that it remains suitable and appropriate to the business as the business grows and changes.

Running a small business involves the assumption of risk. Don't assume more risk than is necessary; make certain you have an appropriate insurance program in place to cover losses.

Other Measures

Should disaster strike your small business, you will likely need extra funds to cover uninsured losses until your deductible is reached and you may incur additional expenses in activating alternate business sites and paying expenses until your insurance company pays your claim. We learned an unusual variant of this lesson on September 11, 2001. Many people carry little cash on their person to minimize the risk of loss due to theft and perhaps to impose spending discipline. On September 11, when workers and residents of Lower Manhattan had to evacuate their work premises, many found that they could not obtain cash from ATM machines and their normal commute home was disrupted. My banker (Donna), who lives in New Jersey, had to walk on foot across the Brooklyn Bridge and then needed funds to get home to New Jersey, since the train she ordinarily took was not in operation. It took some time before she could find her way home. We now keep some petty cash in the office for emergency use. It seems trivial to consider this, with the easy availability of electronic funds, but when you experience the inconvenience of being stranded, you want to ensure that it doesn't happen again.

We recommend that you take steps to ensure access to capital while your business is running smoothly in the normal operating environment. You may wish to put in place bank lines of credit or obtain higher limits on your credit cards while business is functioning smoothly. After a disaster strikes, you may have greater difficulty obtaining credit. Your customers may be slower in paying their obligations to you, which in turn

may hinder your ability to pay your obligations and may create blemishes on your credit report. Having pristine credit will help you obtain disaster-relief financing, which is typically offered in the form of loans.

Having access to capital may give you the funds you need to keep your business operational during the period of time required to complete a disaster loan package and await disbursement of funds. The old adage applies here: the best time to apply for a loan is when you don't need one. Apply for credit lines in the course of your normal operating environment that will be available to you when disaster strikes. Finally, we urge you to do what you can to build a cash reserve sufficient to meet three to six months' operating expenses. It is difficult when you are launching a business to accumulate savings, so we budgeted for business savings, just as we planned for ordinary capital expenses, until we reached a cash reserve figure that gave us peace of mind. Even if disaster never strikes your business, the discipline of risk management and financial planning will improve your business processes.

NOTES

1. Institute for the Future, "Workplace Communications in the 21st Century Workplace," study conducted for Pitney-Bowes, May 1998.
2. Even during the World Trade Center attack, cell phone service continued with little interruption. But you might expect the cell phone network to be easily overloaded when land-based phone service fails. It is therefore a good idea to have several cell phones from different providers available as part of your contingency planning.
3. Services on the website are available for this purpose: *www.getconnected.com* and *www.lowermybills.com*. You enter your telephone area code or zip code and the service generates charts of available services in your area—long distance, wireless, Internet, and gas and electricity—sorted by price.