
August 11, 2005

Trying to Stay a Step Ahead of Murphy's Law

By EVE TAHMINCIOGLU

Don't put it off any longer.

That is the advice of specialists in planning for disasters, who say too many small businesses are courting ruin by failing to take fuller precautions against fires, floods and, increasingly, the loss of critical data stored in computers that go on the fritz.

Jane Vitart wishes she had acted sooner. When the Delaware River overflowed behind the French bakery and cafe she owns with her husband, Joel, in New Hope, Pa., last September, a retaining wall protected her shop. That lulled the couple into a false sense of security, and when the flood waters rose again in April, they did not bother to evacuate their equipment or their computer as they had seven months earlier.

Big mistake. "The river rose four feet higher than it did in September and we ended up with 31/2 feet of water in our bakery," Ms. Vitart said. "The kitchen, the store, my entire office was destroyed. This time the river took that retaining wall."

The flood caused about \$120,000 in damage and clean-up costs, but perhaps the biggest blow was the disabling of her computer under three feet of water. "I ran my whole business on that computer - all my financial data, inventory, vendor bills, my marketing materials, customer lists, menus," she said. "I was even working on a Web site and had all the photos I had taken on there." It wasn't as if she hadn't taken defensive measures. She had backed up a lot of her financial data, but the backup disk turned out to be defective and she was unable to retrieve the information.

Ms. Vitart's adversity is being repeated with increasing frequency across the world of small business, specialists say. Entrepreneurs, who are often short-staffed and consumed by the problems of the moment, have always been a bit haphazard about preparing for unexpected events that could threaten their firms' survival. But the technology revolution that has made them reliant on computers for storing information and running their companies has made vigilance all the more crucial, contends William G. Raisch, executive director of the International Center for Enterprise Preparedness at New York University, which is financed by the Department of Homeland Security.

That data can be lost in fires, floods, burglaries, computer malfunctions, virus infections, even terrorist attacks, Mr. Raisch said. "The reality is that small and medium-sized businesses have less of a capacity to recover from these things because they are generally concentrated in a single site and some disasters can go well beyond their resources," he said.

Entrepreneurs can hardly be unaware of the dangers. A survey of small-business owners conducted last year by the Gallup Organization for the Research Foundation of the National Federation of Independent Business found that at least 30 percent of respondents had had to shut down for 24 hours or longer in the previous three years as a result of a natural disaster, like a blizzard or hurricane. One in 10 reported hardship from man-made disasters like civil disorders or arson.

And more than one-third said they had been victims of computer viruses; of those, 28 percent had lost data, 29 percent had had to buy new equipment and 60 percent had had to hire outside help to fix the problem.

The sudden breakdown of a computer system can inflict harm beyond just the loss of data. More and more

large companies are asking their suppliers to connect with them electronically for ordering and inventory control, so a disruption of Internet access even for short periods can jeopardize a small business's relationship with clients.

What concerns small-business experts is the continuing resistance of so many entrepreneurs to bite the bullet and take action. Consider Ms. Vitart's course of action after the flood nearly destroyed her business. She and her husband shut down the bakery for six weeks, losing an estimated \$50,000 in sales, and reopened it the week after Mother's Day only by stretching their credit to the limit and using all their personal savings. "I feel like I'm starting from scratch," she said.

The couple made some changes to make it easier to cope with future floods, like paying a carpenter to rebuild the shop's counters in small units to make them easier to remove. In the future, she says, she will evacuate her computer at the first hint of flooding. But she has no plans to hire a disaster recovery consultant or purchase a service to protect her data.

Some specialists say she ought to consider some additional steps. Yossi Sheffi, director of the M.I.T. Center for Transportation and Logistics, said small-business owners like Ms. Vitart should at the least make sure their backup disks are functioning by testing them periodically. He also advised business owners to buy firewall protection and antivirus software, and to consider investing in an off-site data backup service.

And do not take anything for granted, he advised. After hiring a firm to store data, business owners should contact the company about three weeks into the process and make sure all their information can be easily retrieved. That means having the company either send a disk with the data or give access to the data online.

Mr. Raisch of New York University counsels small-business owners to review their important business processes and understand what the business relies on. He suggests reading NFPA 1600, a preparedness standard from the National Fire Protection Association that grew out of an effort by the Federal Emergency Management Agency in the early 1990's to create a common backbone for emergency planning. The standard was given a lift in July 2004 when the 9/11 Commission urged its adoption. It offers businesses of all sizes a benchmark and guide for planning everything from protecting employees' safety to identifying natural, human and technological disasters. Copies can be downloaded at NFPA.org.

Many small businesses have learned the hard way to take steps to protect the stored information that is their lifeblood. Riza Chase-Gilpin, owner of Kitty's WonderBox, a Wellington, Fla., maker of disposable cat litter boxes, was hit with a computer virus last year when she opened an attachment from an unknown source. The virus shut down her only computer and she was unable to gain access to customer information or to place orders on the electronic data interchange, known as E.D.I.

"We ended up being late on a couple of deliveries because we couldn't do E.D.I.," she said. "I had to call the E.D.I. company I work with and ask them if any orders had come in and then they would fax them to me. We missed a couple of orders as a result and that could have had a huge financial impact."

Luckily, when she explained the circumstances to her customers, they were sympathetic. Fixing the computer cost Ms. Chase-Gilpin \$600, but she bypassed a larger expense because she had all her information, including invoices and purchase orders, on hard copy. She bought a laptop in January so she's not reliant on a single desktop computer, and she added full virus protection on her computers at a cost of \$150 annually.

Time is also a critical issue for small businesses. Two years ago, sorting through the spam pouring into the e-mail directories at Shustak Jalil & Heller was wasting upward of an hour a day of the partners' time. Given a billing rate of \$300 an hour, the wasted time was becoming a financial burden on the law firm, a boutique firm with offices in New York and San Diego.

"In our business, the only thing we have to sell is our time," said Irwin Shustak, managing partner. The

solution was quick and cheap. Mr. Shustak turned to a consultant, and based on his advice, subscribed to a spam-and-virus filtering service for \$500 a year. As a result, he said, "We've cut down on virtually all of the junk mail."

[Copyright 2005 The New York Times Company](#) |