The Wall Street Journal, September 27, 2005

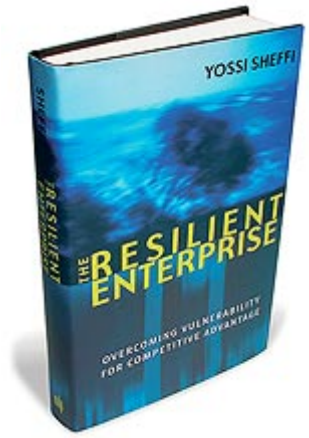
Books

What to Do Before Disaster Strikes

By GEORGE ANDERS

A century ago Lord Leverhulme, the British soap tycoon, remarked famously: "Half the money I spend on advertising is wasted. The problem is I don't know which half."

Today's executives could say much the same about their outlays for security services and disaster preparedness. Since the terrorist attacks of 2001, companies have feverishly tried to shield themselves against a thousand versions of the unthinkable. There is a lot to be scared about, and no shortage of ways to buy protection.



Jason Huff/The Wall Street Journal

It's not just bad weather that businesses must prepare for. Catastrophe lurks in many forms.

What's missing is a systematic way of approaching corporate self-defense. Each potential calamity is treated in isolation. Earthquakes, floods -- and certainly hurricanes -- can threaten corporate assets. Computer hackers can target vital databases. Anthrax can show up in the mailroom. Bosses feel obliged to treat each peril seriously. Yet there is an understandable reluctance to hand over more money each time a consultant hawks an alarmist story.

In the midst of this scramble for safety comes Yossi Sheffi, professor of engineering systems at the Massachusetts Institute of Technology. In "**The Resilient Enterprise**," Mr. Sheffi sets forth some wide-ranging ideas about how companies can stay one step ahead of trouble. He doesn't have all the answers, but at least his perspective is broader than that of the crisis-of-the-day brigades.

Mr. Sheffi believes that companies need to start by cataloging what could go wrong. General Motors Corp., for example, has created "vulnerability maps" that identify more than 100 hazards, ranging from wind damage to embezzlement. Such maps make it easier for managers to focus on areas of greatest risk or gravest peril. He implies that normal budgeting -- which matches the cost of doing something against the risk-adjusted cost of doing nothing -- can determine which battles against vulnerability are worth fighting.

He may be right. Still, he misses an opportunity to talk more explicitly about the danger of overspending on remote dangers. (There is a point at which even the most safety-minded company needs to say: "Enough!") Instead, "The Resilient Enterprise" rolls into dozens of case studies involving both famous and obscure misfortunes. These range from

the Bhopal, India, chemical spill in 1984 to the theft of Intel Corp.'s Pentium chips at London's Heathrow Airport in 2003. His dissections move along with such brisk energy that they become surprisingly good reads.

Details

THE RESILIENT ENTERPRISE
By Yossi Sheffi
(The MIT Press, 338 pages, $29.95)

Early on, Mr. Sheffi recounts how a minor fire at a Philips NV microchip plant in New Mexico caused huge disruptions in cellphone assembly for months afterward. One customer, Finland's Nokia Corp., quickly mobilized other sources of supply and kept its production lines running. Another customer, Sweden's LM Ericsson, didn't move as fast and incurred losses of more than $400 million. Ultimately, Nokia ended up with an overpowering market-share advantage over Ericsson, which was forced to bring in a partner, Japan's Sony Corp., to keep its cellphone business alive. As Mr. Sheffi tells it, the two phone companies' divergent fortunes "were set well before the fire hit," simply because their crisis-response strategies were so different.

Mr. Sheffi nods approvingly at some ingenious ways to mobilize for trouble before it arrives. Federal Express Corp., he says, puts two empty planes in the air each night, just so they can swoop into any airport with a grounded plane and take over delivery services as fast as possible. Wall Street firms have recently added similar redundancy with multiple data centers, so that a New York City crisis won't imperil their record-keeping.

Intel Corp. (post-Heathrow) gets a thumbs-up, too, for finding a sly way of outwitting airport thieves. It couldn't control every aspect of security in transit -- but it could change its box design. Rather than boast about "Intel inside," the company switched to drab, unmarked packaging that gave no hint of $6 million cargoes. The name for this approach: "Security through obscurity."

After writing in an omniscient voice for most of his book, Mr. Sheffi explains in his end notes that many details of his case studies come from the business press. For his opening account of the chip-plant fire he borrows heavily, footnoting a single piece from the New Mexico Business Weekly six times and citing a front-page article from this newspaper 13 times. It wouldn't have hurt to acknowledge these sources in the main text as well.

Overall, though, "The Resilient Enterprise" is more than a grab bag of stories about fires, thieves and tornadoes. It is the timely analysis of an important -- and overlooked -- aspect of business strategy. Mr. Sheffi argues that crisis control can be a competitive advantage for companies that get it right. Wise planning at headquarters is part of the answer, but only part: Companies need a whole culture of flexibility. It is impossible to know where trouble will hit next, but it is possible to create an atmosphere in which people at all levels respond to disruptions quickly and confidently. Metaphorically, levees can break at any time.

Mr. Anders is a news editor in the Journal's Palo Alto, Calif., office.

Once disaster strikes, every decision you make will have an effect on whether you survive or not. Making the right call will keep you and your loved ones alive. Failing to take immediate action and not using all the information you have, will drastically lower your chances of survival. When disaster strikes, you have to be ready and you have to know what to do. The most critical decision you must make is if you stay or if you evacuate. The sooner you know what to do the better you will be. Taking a decision when disaster strikes. To decide if you need to bug out or if you need to bug in, you n The key to averting disaster or minimizing its effects is a solid data security plan. Learn the types of data risks that exist, how to develop a plan to counteract them, and your role in ensuring the safety of health and patient data. Do you want to read the rest of this article? Request full-text. Advertisement.Â Disaster recovery planning (DRP) is many things to many people. To some, it is planning how to recover or replace damaged computer systems in organizations that range from a single nurse practitionerâ€™s office practice to a multisite hospital group. To others, it is planning how to maintain critical hospital/nursing functions during interruptions in computer service. Do you know how to actually protect yourself during an earthquake or hurricane? What about a tornado or fire? You've probably heard lots of conflicting information over the years.Â For Any Disaster: Make a Disaster Preparedness Plan. One common thread you'll see in almost every section below is that you'll need a disaster plan. You should be familiar with it before the disaster, and ready to act on it in case the unthinkable happens.Â However, because earthquakes can strike suddenly and without warning, and in some cases they can lead to other problems like fires or tsunamis, it's critical to have a disaster plan for your household and family, and to have practiced it so it's second nature when you need to act on it. Give your home an earthquake checkup.