Photograph by Steve Edson

Yossi Sheffi: The Thought Leader Interview

Truly resilient companies treat security as an integral part of their strategy, says MIT's leading supply chain expert.

by Amy Bernstein

Few issues have morphed as dramatically in the last five years as corporate resilience. That phrase once referred to managing risks that were fairly predictable and relatively easy to insure against: fires, strikes, and economic recessions, for example. But all that has changed. A string of catastrophes — beginning with the terrorist attacks on September 11, 2001, and continuing through the bombing of the Madrid railway and the Asian tsunami in 2004, the blast on the London Underground in July 2005, Hurricanes Katrina and Rita in August and September, and the earthquake that devastated Pakistan in October 2005 — has rearranged our concept of disaster preparedness. It's no longer enough for companies to devise a business continuity plan and file it away somewhere. They now have to figure out how to bounce back from the unthinkable.

The leading proponent of that argument is Yossi Sheffi, a professor of systems engineering at the Sloan School of Management at the Massachusetts Institute of Technology, in Cambridge, Mass. His specialty — the management of logistics and

Amy Bernstein
(bernstein_amy@strategy-business.com) is deputy editor of *strategy+business*.

supply chains — has taken on heightened significance in a world that is increasingly globalized, complex, and vulnerable. His new book, *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage,* published in October 2005 by MIT Press, is burnishing his reputation as a leading expert on corporate durability. "Resilience is not a company issue; it's a supply chain issue," he explained over coffee in his office at MIT, "because a company can get disrupted not only if one of its plants is hit, but also if the capacity of a crucial supplier is disrupted, or if a big customer is disrupted."

According to Dr. Sheffi, the attacks of September 11 provoked him and many of his colleagues to seek a more sober, comprehensive, and probability-conscious view of risk and resilience. "Before that, I thought about it mostly in financial terms — buying insurance against various business risks, buying commodity futures such as oil to hedge against price fluctuations, the use of financial derivatives, et cetera. In the wake of the attacks, I started looking at all kinds of disruptions, and it became clear that there's a lot more to consider than contingency planning or financial hedging. There are low-probability/high-impact events like terrorist attacks that may cause unplanned exits from important markets or even the demise of the unprepared business."

How enterprises rebound — or fail to rebound — from those events became the subject of a three-year study that culminated in his book. Dr. Sheffi and his colleagues examined dozens of organizations, from Toyota to UPS to the U.S. Navy, and drew a simple conclusion: A company's ability to return to business depends more on the decisions it makes before a shock hits than those it makes during or after the event. He explains why, for example, a fire at a Philips chip plant in New Mexico inconvenienced its customer Nokia, the cell phone maker, but staggered Nokia's long-time rival Ericsson. The key was that Nokia's culture encouraged constant communication, so the company reacted immediately and was able to source its chips elsewhere. Ericsson, by contrast, responded slowly and was left high and dry. By building flexibility into the entire supply chain, says Dr. Sheffi, companies can tame their risks and gain competitive advantage.

But all that is easier said than done. Dr. Sheffi worries that corporate security has not caught up to the realities of doing business today. The more complex a company's supply chain, the more vulnerable it is to every kind of threat, from lightning strikes to theft to terrorist attacks. To guard against disruptions of all sorts, companies must approach security "holistically," as a factor that affects the entire corporation and requires attention up and down the supply chain. In this interview, conducted in October 2005 with *strategy+business,* he explained how to do so.

S+B: Describe the state of corporate risk management today.

SHEFFI: Risk management is where some other corporate functions used to be in the '80s. It's a standalone, with people working in three separate parts of most companies. First, there are the business continuity people who, once every so often, come up with a plan that then sits on some shelf until it's called for. Second, there are the security staff, who are basically the "guns, fences, and dogs" people. They decide who needs a pass to get in and out of the building, and when employees go to certain countries, they make the

travelers read the CIA country reports and the latest State Department warnings.

Third, there is the information technology piece — securing firewalls, updating antivirus software, and recovering data if there is a disaster. Any modern corporation that loses its financial records, customer records, or transaction records will probably go out of business. But risk management strategists never had to spend a lot of time on this, because there's an easy fix — build redundancy into information technology — and most companies have done it already. After 9/11, for example, most of the financial-services companies that were housed in and around the Twin Towers were able to start operating when the Exchange reopened a few short days after 9/11. They already had fully functioning trading floors and access to their records on the other side of the river, in New Jersey, with phones and computers, and they just went to work.

What worries me is that these three stand-alone functions are not incorporated in corporate strategies, not integrated with the business, and therefore not treated with respect within the corporation. They're not a traditional way station on the path to the CEO office.

S+B: Why is that a concern? Why shouldn't security be treated like any other overhead function?

SHEFFI: Because the traditional definition of security and business continuity is but a small part of true resilience. A real strategy to mitigate risk doesn't just mean having better dogs and guards and electronic passes or business continuity plans in case disaster hits. It means that the entire company is more flexible up and down the supply chain. It means that suppliers, customers, the trucking companies they use, the forwarders they use, the custom brokers, and every vendor to every part of the business is being fully integrated with the enterprise and able to respond fast to changes.

To accomplish this, a company may have to redesign its products, redesign its processes, and keep doing it. It's not a one-time event. We know that companies have to continuously look at the risks that they face, and that they need better tools to do it. Certain supply chain designs provide better flexibility and agility, and can respond more effectively when conditions change.

All of this requires people who are seen as critical within the company and potential leaders of the whole enterprise. They have to be business professionals who don't just push for more investment in resilience, but who can balance security and resilience needs with the other goals of the enterprise.

S+B: You say that there are better supply chain designs. What do they look like?

SHEFFI: One important feature is interchangeable parts. Companies should avoid using parts that are engineered to purpose. Of course, that's heresy to an engineer like me. We get our satisfaction from designing something that is 0.003 percent better than the other guy's design, that is specifically designed for a specific purpose and does its job perfectly. But being "good enough" creates many benefits. It's better if a part can be used for multiple products, because then it is easier to forecast the need for parts, since the manufacturing process depends less on the vagaries of the demand for any single product. Parts can be sourced from several suppliers because so many are needed, or they can represent a crucial business for a single supplier who will give greater attention to the company's needs. The inventory turns for such interchangeable parts are higher, allowing for higher availability; and any problem with one of the products does not cause the company to be "stuck" with a special-purpose part that has no other use.

But it isn't just parts that should be designed to be interchangeable. Intel has a practice that they call CopyExact. You walk into one Intel plant, say in Israel, and then into a second Intel plant, say in Malaysia, and you get a feeling of déjà vu. The two plants are eerily identical. They are even positioned the same way relative to the sun. This practice did not start as a resilience strategy. In the early days, engineers couldn't figure out why sometimes they got great yields and sometimes the yields were low. So once they got it right, they started copying things exactly. But the benefits went beyond getting the manufacturing process down right. During the last severe acute respiratory syndrome [SARS] outbreak in 2004, for exam-

ple, Intel was able to move production around with little trouble. Because all fabrication plants are identical, they can manufacture everything everywhere.

Another example that's close to everybody's heart is Southwest Airlines. It uses only 737s. When Boeing came up with a glass cockpit that was all digital, Southwest executives took one look and said, "We'll use it. But you boys go back and reprogram the glass cockpit to look just like the old steam gauges, because we want every pilot to walk into every cockpit and be able to fly it." Fungibility is vital with staff, just as it is with parts. This is an important principle in supply chain design: If you avoid the need for specific people or parts for specific purposes, you create flexibility.

S+B: How else do you build in flexibility?

SHEFFI: Another important principle is "Delay the decision": put off customizing the product and keep it in a semifinished state as long as you can. Hewlett-Packard makes printers for Europe in Singapore and Vancouver. Invariably, in the past, they found themselves stuck with too many Slovak printers and not enough Danish printers. So several years ago they changed their supply chain to make "vanilla" printers with all the internal workings — which don't change from market to market — but without the power supply, plug, decals, and instruction manuals. They send everything in its vanilla state to a distribution center in Holland, and once they get an order, they slap on all the appropriate decals, plugs, et cetera, in the distribution center. The packaging was even redesigned with a side panel so HP can perform the country-customization operation without opening the box. They claim millions of dollars of savings based on this.

All that means is that if there's a disruption downstream, you won't suffer as much. Let's suppose there is a strike in France. That's not a low-probability event, obviously. But while nobody's buying printers in Paris, HP won't get stuck with mountains of French printers. Those printers will go to Denmark or England. Maybe they will even run a sale somewhere else. But they can do it, because they haven't yet made the printers French.

Dell is the ultimate example of postponement with their build-to-order supply chain and manufacturing design. Their suppliers hold on to the parts for Dell computers until an order comes in. Only then does Dell pull the parts in, build the computer, and ship it to the customer — all within a few days. Why is this important? In 1999, there was an earthquake in Taiwan that knocked out about 40 percent of the world's chip supply. At the same time, both Dell and Apple were coming out with new models. Most people don't realize that Apple also makes computers to order — it does not build a computer until it has an order for it — but its operation differs from Dell's in one crucial aspect. To gauge demand for the model they were introducing that year, Apple published the specifications on their Web site and started taking customer orders — a quarter of a million orders by the time they started manufacturing and shipping the computer. A week after they started shipping it, the earthquake hit. Now, Apple had about 250,000 orders on hand for a specific configuration at a specific price, which it could not fulfill. So it tried several things, including sending its customers less-powerful computers. That backfired, erupting all over the media, and they had to take many of the computers back. Many of the orders evaporated.

Dell, on the other hand, doesn't have a six-month backlog of orders. Dell takes an order and builds the computer. When the earthquake struck, Dell changed the prices on its Web site. The configurations that they couldn't build because they didn't have the right chips were suddenly more expensive. The configurations for which they did have the components were less expensive. To keep the prices low on some models, Dell announced that it would ship those configurations with less memory. Dell shaped the demand to where it could fulfill it, unlike Apple, which was stuck with long-term commitments to specific configurations. [Also see "Manufacturing Myopia," by Kaj Grichnik, Conrad Winkler, and Peter von Hochberg, *s+b*, Spring 2006.]

S+B: How does this kind of thinking fit with service firms and nonmanufacturing enterprises?

SHEFFI: There are a lot of issues around the deployment and train-

"When an ice storm shut down Louisville roads, UPS cleared its runways and flew in workers from Atlanta."

ing of employees. You can redesign operations into a series of small processes on which the employees — and even the suppliers — can be trained, so that if there's a problem, work can easily be moved around. In 1986, a big ice storm shut down Louisville, where UPS has a major hub. UPS workers couldn't get out of their driveways to come to work. But the company realized that while they couldn't clear the roads, they could clear the runway, and they started flying workers in from other parts of the UPS system. An employee in New York or Atlanta could do the work in Louisville because the systems are relatively standard, and because the employees are cross-trained.

Cultures of Resilience

S+B: Is there an essential difference between companies that respond well to disruption and those that don't?

SHEFFI: It was clear from our work that there's something in the DNA of companies that are resilient that doesn't seem to exist in the DNA of companies that are not so resilient. In the study that led to *The Resilient Enterprise,* my colleagues and I referred to this element as "corporate culture," and we tried to analyze its characteristics.

We found that resilient companies communicate obsessively. Every Dell manager gets a production report of what's happening throughout the company every two hours. They get it on their PDA or pager — so they're always in the know.

Another important principle of resilience is "Drive the power to make decisions down in the organization." Most people are familiar with the way Toyota empowers production-line employees to pull the *andon* cord and stop the line if they spot a quality problem. [The *andon,* from the Japanese word for *lamp,* is a visual display that lights up when a sensor detects an anomaly on the assembly line.]

Zara and World — two retailers based in Spain and Japan, respectively — are unbelievably good at empowering line employees. In both companies, the store managers collect information every night, not only about what is selling and not selling, but about why it is not selling. They interview customers. "Why don't you buy this shirt?" "Can you please tell me what's wrong with this blouse?" They get all this information and report it every night to headquarters. Computers sift through this information and try to find out if there's a certain trend. The same night, designers, who are mostly 22- to 25-year-olds, sit in front of their computers and change the designs on the screen, send it on their own to manufacturing, and it goes from there back to the stores. It takes them three weeks to go through the whole process. This is something that takes Marks & Spencer nine months to do.

The reason the system works so well is that there's no approval process. Those designers do it basically on their own. Sure, they make mistakes, but the system is so fast that it's clear very quickly what the mistake was, and three weeks later it gets corrected.

S+B: I imagine it makes a difference in the attitudes of people who work there.

SHEFFI: In resilient companies, you always find passion for the work. In the book, I quote an executive from Southwest Airlines who said, "We're trying to take the bricklayer and convince him or her that they are building a cathedral." Navy seamen don't think about their job as driv-

"A very good company is naturally resilient; it is flexible and can respond to the marketplace."

ing big ships. They think about the job as defending freedom. Dell refers to the attitude of its employees as the "see the hill, take the hill" mentality. If there's a challenge, attack it. Don't ask for permission. Just do it.

Passion starts with understanding the mission of the entire company, being part of the mission, and buying in on it. You understand the greater goals of the company, and you care. If there's a danger to the organization, you'll go out of your way to help.

Instilling this level of passion requires obsessively communicating what the company is about, what's going on, and what challenges it faces. UPS, for example, broadcasts all its weekly management meetings to the entire company.

The simple fact is that resilience grows out of communication, passion, flexibility, and agility, and they are all tied together. A very good company is naturally a resilient company, because a very good company is flexible and can respond to the marketplace. A very good company will have all its functions and people aligned with its mission, with its vision.

For the best examples, look for companies that operate in very uncertain markets — consumer electronics, high technology, fashion, and service organizations. In consumer electronics and high tech, the rate of change of the product is so fast that the uncertainty in terms of demand is huge. You have to design a responsive supply chain to fulfill the market demands yet not get stuck with surplus inventories. The fashion industry is another example; it changes with the whims of teenagers in unpredictable ways, forcing companies to adapt quickly. These companies find it relatively easy to build in flexibility for disruption recovery because, at the core, a supply disruption and a demand spike are not all that different. In each case there is not enough supply to meet the demand.

Service companies like UPS, FedEx, and American Airlines are also models of resilience. They cannot accumulate an inventory of their product, so a disruption means lost sales without a chance to recover by selling the product later. In addition, many service companies' operations are affected by weather, road construction, crime, and other environmental phenomena, giving them continuous drills in disaster recovery. Many of the best practices for building flexibility and the ability to recover quickly from disruptions were developed by service companies.

S+B: What about companies outside those industries?

SHEFFI: Companies that don't have a lot of practice in this, like manufacturing companies, can insert uncertainty into their operation. Intel, for example, will do a Red Team exercise. They'll come to a plant and tell the plant manager: "You know this part that comes from your number-one supplier? Well, that supplier just had a fire, and now that supplier is gone. What do you do now? How do you recover?"

The difference between having a business continuity plan and this process is huge. Think about the fire drills you had when you were in school. Nobody gave you a little piece of paper and said, "In case of fire, do that." They said, "OK, there's a fire, and everybody go outside." You actually conduct the exercise, you get to understand what to do, and you see if there are problems with the plan before it's too late.

Corporations also have to make sure that they don't protect only

against the obvious, or only against things that happened in the past. Have a team of your employees who know your operation try to attack your facilities. The armed forces, of course, do this all the time. They have one tank battalion "fight" another, and they try to learn from this. There are many ways of doing this. I know of a Quaker plant that has monthly contests in which they put a package somewhere. The employee who discovers the package first gets a prize and is celebrated in the company newsletter. There's another lesson here: Quaker recruits their entire work force to be part of security, creating a "citizen watch."

Offshore Uncertainty

S+B: How does globalization affect your thinking?

SHEFFI: The globalization of business introduces its own risks and uncertainties. First of all, lead times grow. So we have to forecast further in advance. And one of the basic truths about forecasting is, the longer the period you have to forecast, the less certain you are about the outcomes.

Second, globalization brings a lot more participants into the supply chain. These include foreign manufacturers and their supplier networks, foreign transportation and port operators, and myriad government regulators. The global network of participants is not always transparent and there are many more opportunities for theft, accidents, use of substandard labor practices, and terror, so you introduce a lot more uncertainty on both the demand and the supply side.

Currently, in some industries, the difference in the cost of labor is such that they have no choice but to outsource to, say, China. But in other industries, the choice is not always so clear. My feeling is that in many cases not all costs in terms of increased risks are taken into account. One of the problems is that we don't have good metrics for operational risks. If a company engages a supplier in China to do something, there's no way to quantify that this company went from 0.71 to 0.73 on some sort of risk index or operational risk ratio. The appropriate metrics don't exist yet.

Some managers have a general awareness of risk. Clearly they know that taking a supplier in Indonesia is not like taking a supplier in Kansas City. It's easier to keep tabs on what's going on in Kansas City than in Indonesia. But there's no way to quantify the difference. So people make the decisions based on what they can quantify, and what they can quantify are labor costs, landed costs, or whatever the knowable cost might be. And since financial analysts also lack the tools to quantify the increased risk, this is not reflected in the stock price. My feeling is that much of the offshoring is done without proper comprehensive analysis of the consequences.

S+B: Is there a role for public–private partnerships?

SHEFFI: Very much so. It happens at all levels. Let me give you a small example at a local level. Intel has a plant in Oregon that sits right on a fault line. If the plant shuts down, Intel stands to lose about half a million dollars for every hour that the fab stands idle. Even though Intel built the plant to withstand a catastrophic earthquake, state regulations prevent Intel employees from returning to the plant until it passes inspection. But the local government isn't likely to rush its inspectors over to the Intel plant after a quake; they're going to send them first to schools and hospitals and get those up and running. So Intel trained a team of its employees to be inspectors and got them certified by the state. They have an agreement with the state that in case of an earthquake, this team will inspect the Intel plant first, and then will help the city and inspect the hospitals and the schools. It's a perfect example of how government and industry can help each other.

The Technology Asset Protection Association (TAPA) is another example. Millions of dollars in Intel chips were routinely stolen as they were being shipped through airports. So a group of about 500 companies — Intel, Sun Microsystems, and others — formed TAPA to share their wisdom on freight and cargo security. They looked for better ways to audit truck lines, steamship lines, and other transportation suppliers. It started with antitheft, and after 9/11 it became antiterrorism. TAPA worked closely with local authorities in Great Britain to nail the gangs that were orchestrating the Intel chip heists. It's thanks in part to TAPA that Heathrow Airport is no longer known as Thiefrow.

The U.S. Bureau of Customs and Border Protection actually adopted TAPA's 70-point security checklist when it came up with its Customs-Trade Partnership Against Terrorism program. C-TPAT asks companies to comply with certain guidelines and share certain data in exchange for moving their shipments through U.S. ports faster. Using that information, C-TPAT seeks to identify outliers from certain established patterns of ship-

ment. C-TPAT–certified companies agree to implement certain security processes themselves and to demand that their suppliers do the same. The rewards for certification are significant: It can cut the pass-through time for companies from two weeks to two days. That in itself was enough of a draw for fashion companies, like Limited Brands (the parent of Victoria's Secret and other brands), to be active partners with the government.

S+B: You've described where we are now in terms of risk management. What does the ideal state look like?

SHEFFI: In an ideal world, risk can be quantified. The quantification of risk will always involve uncertainty, because we'll only be able to point to the probability of something going wrong. But having metrics that are continuously updated to reflect the state of the world will lead to better-informed decisions. You won't decide to go to China just because your competitor's going there. You'll do your analysis, understand how such a move will increase your risks, and maybe put some reserves against it or increase your safety stock.

I'll give you an example. In 1998, Hurricane Mitch destroyed Unilever's Q-tip plant in Puerto Rico, which was responsible for half the Q-tip supply to North America. Unilever decided not only to rebuild that plant, but, to cut costs, to move 100 percent of their production there. They realized that they were taking on more risk, so they increased their inventory. Now they keep 10 percent more safety stock in the United States. Accounting for the increased risk means more inventory, which means higher costs, but in the final analysis Unilever deemed the move justified.

That kind of decision is based on the kind of holistic analysis that you usually don't find in corporations. You know why? In many cases, manufacturing and inventory management are two separate functions in the organization.

I'd like to see organizations doing holistic analyses of the total risk to the enterprise more often. Because, in many cases, mitigating one risk creates another. For example, companies may disperse operations in order to avoid a concentration risk where a single point of failure can shut down the entire enterprise. This creates another risk: increasing reliance on communications, which creates vulnerability to communication system failures.

Ralph Lauren pushes all its garments for the North American and European markets through a distribution center in High Point, North Carolina. The garments might go from China through the port of Los Angeles, on to North Carolina, and then back to a store in L.A. They do this to protect the brand by ensuring that all stores get a new product on exactly the same day. But if something happens to this distribution center, the company may find it difficult to recover quickly. So while they worry about managing reputation risks, they create another kind of vulnerability. Companies often push risk from one division to another and from one type of operation to another, rather than try to have a holistic understanding of it throughout an enterprise or supply chain.

Now, some companies do think about risk and do a lot to prepare. I recently met with a leading financial-services company that has its own stash of Tamiflu and is laying out plans for how they'll work people from home if there's an avian flu epidemic. They're actually having their people talk to suppliers to

assess which will keep operating in case of an epidemic and which will not. That same day I met with another company, in the same industry. That company views the possibility of the avian flu as a force majeure and has decided to do nothing about it. They're not oblivious to the fact that avian flu may be coming, but their attitude is: "Whatever happens to the population happens to us."

S+B: In a state of better risk management, where both enterprise and government take a holistic approach, how will our lives change?
SHEFFI: Let's start with what it does not get us. It does not get us freedom from disruption and disasters. This is life. There's no 100 percent security and 100 percent certainty about the future. It's just not in the cards.

But it does get us more informed decisions. For example, suppose you're a consumer. You're buying a toaster oven for 50 dollars, and somebody's trying to sell you insurance for this toaster oven for, say, 15 bucks. Most informed consumers would not buy this insurance, because you know that there's not much chance that the toaster oven will break, and even if it does, you're only out 50 bucks. It's not going to be a disaster.

On the other hand, most well-informed people buy health insurance. They don't buy it because there's a strong probability that they'll need it — in fact there's not, and that's why insurance companies make so much money. But the consequence of not having it can be so bad. You buy health insurance because you want to eliminate certain really bad risks if you become sick or get injured, like being denied proper treatment or being driven to financial ruin.

When it comes to companies, I'm talking about balancing the various risks against the costs of protection and mitigation. It doesn't mean that decisions and actions taken through a comprehensive process will eliminate risk. It means only that people make decisions with greater awareness of the risks actually undertaken.

Companies will more easily find the "right" level of protection and investment in mitigation measures. The right level is different for every company and situation, but a comprehensive process of assessment and balanced mitigation is likely to lead to fewer surprises.

In the short term, until we have clear models and metrics for assessment of operational risks, companies should involve all functions in strategic decision making and should carefully collect and distill information with Delphi-like processes (synthesizing the opinions of many people) to evaluate risk. They should also be aware of the tendency to move risk around rather than mitigate it. Resilience-oriented decision processes can be coordinated through a senior risk management officer.

In the longer term, as problems persist and trends seem to suggest more volatile markets and less secure and predictable supply lines, research is bound to develop the metrics, methods, and models for comprehensive risk assessment that can and should be embedded in corporate strategy. ✚

Reprint No. 06110