FORTUNE

Weathering Any Storm

In today's volatile world, corporations have to be resilient. That takes a smart risk-management strategy.

In association with:

Council on Competitiveness

Special Advertising Feature
Reprinted from the March 19, 2007

If you want to know the risks a multinational faces, you can look through market reports, SEC filings, and press releases–or you can just read a newspaper. It's a perilous world, and we all know it. Almost every day there are acts of terrorism, pandemics, computer viruses, storms, and other disasters that can whipsaw an organization. But at least there is one upside to all the bad news: Companies can take action, preparing themselves in ways that may not always prevent disaster but can mitigate the damage to their bottom lines. By assessing the risks of today's business environment, they can put contingency plans in place. It's a no-brainer. Right?

Guess again. In fact, most companies are woefully unprepared. Not only don't they understand the day-to-day perils they face, they fail to recognize how these threats can impact their business. That puts them at a severe disadvantage, exposing them to unforeseen events that may hurt them, while at the same time blinding them to opportunities that can spur innovation and success. "Operational risks are increasing faster than companies are learning to deal with them," says Deborah Wince-Smith, president of the Council on Competitiveness, a nonprofit, nonpartisan policy action group in Washington, D.C. "It's a major issue, as Deloitte Research has pointed out, because companies make money by taking risks and lose money by failing to manage them."

The problem, perhaps, is that many companies perceive risk management as a cost center. The conventional wisdom is that you don't make money securing your enterprise. That's why the issue is often relegated to back-office departments like human resources and information technology, overseen by managers who are often buried deep within the org chart. Rarely do top executives or board members tackle risk management directly or factor it into corporate strategy. It's all a blueprint for disaster.

What's needed, says Wince-Smith and other experts, is a whole new paradigm. Call it enterprise resilience: the ability to understand, avoid, and adapt to disruptions while finding new opportunities for growth. Resilient companies don't view risk management as an expense but as an investment which, like quality was also considered a cost until Japanese automakers turned it into a competitive advantage.

Resilient companies know that processes developed to bulk up security can also boost efficiency and the bottom line. They understand that radio-frequency ID chips embedded in goods traveling across the globe don't just deter theft but provide tracking information that lets buyers know exactly where their orders are. The increased customer satisfaction levels that result mean more repeat business, which provides resources for innovation and new products.

A Slow Paradigm Shift

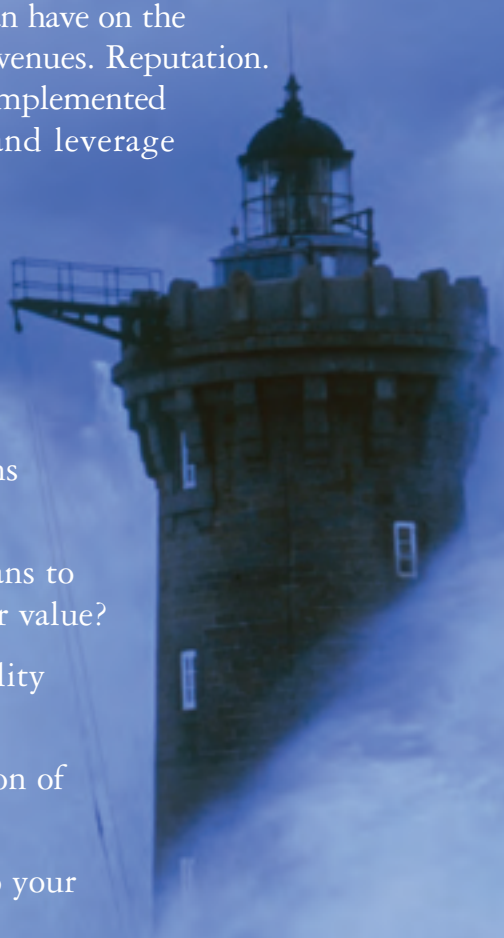
So why hasn't every company embraced resiliency? For one thing, the costs are real from day one, while the payoff is conceptual. So the business case is often hard to make. That may be changing, however—not because the benefits of resiliency are becoming clearer, but because the dangers of not being resilient are.

Consider the potential pitfalls of today's supply chains. They're more global than ever, with vendors scattered across the world. Meanwhile, cost-cutting pressures have spurred corporations to embrace practices like single-sourcing, where they give a lot of business to one supplier in return for a discount. While this lets companies offer their own customers lower prices, it also increases risks. For example, consider what would happen if a tornado ripped the roof off of your sole supplier's factory.

The consequences of supply-chain disruptions can be far worse, and last longer, than you ever thought. In their 2005 study, "Supply Chain Disruptions and Corporate Performance," Vinod Singhal, professor of operations management at the Georgia Institute of Technology, and Kevin Hendricks, associate professor of operations and information technology at the University

Become a Risk Intelligent Enterprise™

When it comes to risk and assessing the impact it can have on the organization, there is much at stake. Customers. Revenues. Reputation. Brand. And shareholder value. Well-designed and -implemented risk management practices can help to protect and leverage these valuable assets.



- Do you have insight into the full spectrum of risks facing your company?
- Does your organization have the resilience to recover from a severe disruptive event?
- Do you systematically include risk considerations in the development of corporate strategy?
- Do you embrace intelligent risk-taking as a means to competitive advantage and increased shareholder value?
- Do you consider both vulnerability and probability in your risk assessment process?
- Do you consider risk scenarios and the interaction of multiple risks?
- Have you infused Risk Intelligent practices into your corporate culture?

Be Risk Intelligent. Visit www.deloitte.com/RiskIntelligence.

Deloitte.

Audit.Tax.Consulting.Financial Advisory.

www.deloitte.com/us

The Risk-Intelligent Enterprise™:

Gaining Competitive Advantage Through Smart Risk Management

Some risks just bring problems: A labor strike shuts down a crucial assembly line; a security breach compromises your customer database. Others, however, can bring opportunities: You bet on an overseas market and hit the jackpot, driving up profits and shareholder value. But deciding which risks to take and which to avoid is tricky—and dangerous—business, particularly today, when competition, pressure to cut costs, and global supply chains bring unprecedented hazards. To find out what makes a risk-intelligent enterprise and how a company gets there, FORTUNE Custom Projects spoke to James Quigley, the chief executive officer of Deloitte & Touche USA LLP, whose subsidiary firms provide consulting and advisory services to help global clients manage uncertainty.

What does it mean to be a risk-intelligent corporation?

It means you don't just worry about the bad things that could happen, like, say, the bankruptcy of a key supplier. You also consider the good things that might occur, like introducing a blockbuster product to the marketplace. Of course, it's important to prevent, mitigate, or recover from all the crises that can occur. But it's equally important to consider risks that are linked to success, so you can capitalize on opportunities. This is what makes companies resilient, able to recover from misfortune, adjust to change, and evolve and grow.

So, just like good cop/bad cop, we have good risk and bad risk?

That's right. On the bad side, you have what we call unrewarded risk. It has no upside. Even if you handle it perfectly, you get no prize in the end. For example, think about workplace safety requirements under OSHA. Failure to comply can only hurt your company; OSHA shuts down your facility for violations. But at the same time, you may gain no extra credit with stockholders for being compliant. Managing unrewarded risk doesn't do a thing to improve your market share or stock price. It simply keeps you in business. Which is why, of course, you have to deal with it.

Chief Executive Officer Deloitte & Touche USA LLP's Quigley

But you also have to deal with the flip side—rewarded risk—right?

You absolutely have to deal with it. Rewarded risk is all about exploiting opportunities for success. Every public company wants to grow and see its shares rise; intelligent risk-taking is what lets them do so. You take a chance—after a lot of careful analysis and thought—and you come out ahead. That's not to say rewarded risks can't have a very large downside; of course they can. But the potential payoff is even greater if the dangers are well understood and managed.

Expanding into new markets, for example, can pay great dividends. But have you taken a hard look at all the uncertainty that's involved? Have you considered the cultural differences? The local laws and regulations your company must abide by? The country's political and social stability? You'd be surprised at how many companies have failed in foreign markets because they didn't think all of this through.

We're seeing a lot of companies suddenly getting serious about managing risk. Why all the attention now?

A combination of forces is at work. Most important is the need to remain competitive in a tough global marketplace. But other forces apply, too,

"Companies have to integrate the principles of sound risk management into every strategic decision they make."

Leaders who are averse to rewarded risk taking find it harder to innovate and achieve long-term success.

such as increased media scrutiny that seems to spotlight every corporate misstep; rising shareholder activism that is forcing boards and executives to be more open and accountable; and regulatory drivers like Sarbanes-Oxley. And added to all this is the speed at which problems can accelerate in the Internet age.

Are companies investing enough to achieve long-term success?

That's an interesting question, because there's certainly no shortage of opportunities out there. Many fortunes are being made—in the Internet sector, telecom, high-tech, and other fields—by companies and investors who took a risk that paid off.

But there's a paradox at work here, too. Over the last few years, business leaders have become increasingly averse to *rewarded* risk-taking. It's understandable, with shareholder activism, turnover in the C-suite, and increased regulation and scrutiny. The evidence is seen in high levels of cash on corporate balance sheets and a widening share of M&A being done through private equity. The danger is that, as a consequence, companies are not going to innovate and achieve long-term success. Managers have to feel a passion to win that is stronger than the fear of failure.

In other words, there is a direct link between risk intelligence and shareholder value?

Growth doesn't come without cost or risk. It requires investment in new, innovative, long-term ideas. Companies have to integrate the principles of sound risk management into every strategic decision they make.

Let's take the example of a consumer technology company that wants to bring a new product to market. To do that, it needs to analyze market trends, size up the competition, devote significant resources to research and development, keep a tight rein on the supply chain, and so on.

All of these activities require the company to understand how to manage uncertainty, identify warning signs, and how it should react. In other words—risk intelligence. There are companies doing this right now, and their shareholder value has risen dramatically.

You would think, then, that Wall Street would be creating market incentives to strengthen risk-management processes.

We see this happening already. Many investor ratings services—like Moody's and Standard & Poor's—now include risk management in their evaluations. These ratings can impact the cost of capital and influence demand for shares in the company. Large institutional investors are also keeping a closer eye on risk management practices within the companies where they invest.

So what can an enterprise do to become risk intelligent?

The first step is to recognize that a lot of sophisticated risk management already goes on within the company. The finance department is effectively managing credit risk; IT is handling security and privacy risks; and so on. The problem is, the people managing these processes don't always talk to or even know about each other. Risks, of course, don't exist in isolation. A privacy risk can quickly turn into a reputational risk which can turn into a litigation risk which can turn into financial risk. So you have to build bridges across the enterprise. Put all of your risk specialists in the same room to have formal, documented discussions about the uncertainties the company is facing and how they should be managed.

Risk intelligence needs to be integrated into all facets of the business, particularly strategy and governance. You need to address risk every time you consider a new acquisition, or enter a new market, or develop a new product.

And you need to fully exploit technology. We often discover that companies aren't even utilizing the risk management capabilities already built into their existing ERP systems.

These steps aren't just useful; they are essential. The perception that the world is an increasingly perilous place is not some radical notion. It's reality. A risk-intelligent enterprise knows when to avoid danger and when to take a chance. It doesn't just stay in business—it prospers. ■

Questions Every CEO Should Be Asking

A resilient enterprise can adapt and change, so it prospers when other companies flounder. But perhaps the biggest change has to come up-front: rethinking the way the organization views and tackles risk. It's no simple task, but these questions will get you started:

- Do we know the overall risk profile of the company's assets—i.e., people, products, processes, and facilities—as well as the interrelationships among these risks?
- Have we integrated risk-management processes throughout the enterprise?
- Are we constantly reviewing and tweaking our business continuity plans?
- Can security processes be improved so the company enjoys fallout benefits—like increased efficiency and improved customer service?
- What technologies and metrics are available to evaluate and improve risk management processes?
- Is adequate security training in place? Investments in firewalls and virus protection don't mean much if no one knows how to use them.
- Do we have an environment where employees feel free to speak out about potential problems to upper-level managers?

of Western Ontario, found that supply-chain disruptions are often catastrophic for businesses and their shareholders. "Companies lost 6% to 7% of their market value on the day they announced a supply-chain disruption," says Singhal. "Then there was the long-term impact: Their shares would underperform their benchmarks by 35% over a three-year period." Singhal thinks that figures like these will get enterprises to change their tune. "People are going to see how serious the issue is and start getting serious about it," he says.

Resiliency, however, isn't just about managing risk so you stay afloat. It's about managing it in ways that let you leapfrog the competition. DuPont, for example, is currently taking one risk—the loss of all the tacit knowledge that invariably occurs when an engineer leaves the company—and tackling it in a way designed to put the company in an even better position. It's putting in place a knowledge-management system: a giant database of know-how that will store much of the invaluable, heretofore uncaptured wisdom that is typically lost when a valued employee departs—all the tips and tricks people learn over the years but never formally document. By making the database searchable, DuPont can use this information in new ways. "With 15,000-plus engineers, we don't always have the ability to communicate efficiently," says James Porter Jr., chief engineer and vice president for engineering and operations at DuPont. "This system will let us leverage and integrate knowledge. People will be able to put two pieces together and suddenly know something new. And that's what will make our company innovative and sustainable."

Recruiting a Champion

The problem is that it is hard to predict—and convince top executives—that a risk-avoidance measure taken now will have all sorts of wonderful re-

sults down the road. "You don't just need to look at the direct benefit of what you're doing, but at all of the indirect and collateral benefits," says J.T. Kostman, an industrial and organizational psychologist and the director of people equity solutions at Metrus Group, a Somerville, N.J., firm specializing in strategic performance measurement. "You need to be a little bit innovative to find these."

Fortunately, there is another way to make the case for strategic risk management: Point to the success stories now beginning to appear. Georgetown University, for example, started taking a hard look at resiliency after the 9/11 terrorist attacks and the anthrax scare on nearby Capitol Hill. It developed an integrated framework for risk management, bringing together security officers, risk managers, and representatives from the university's various business units. Together, they started asking not only how to prevent and recover from disruptions, but how to do so in ways that add value.

"Operational risks are increasing faster than companies are learning to deal with them."

"We quickly discovered that what you do to be resilient can have great benefits on your business," says Spiros Dimolitsas, senior vice president and chief administrative officer at Georgetown. A project to implement dormitory safety standards that exceeded the building code—installing sprinklers and other equipment—resulted in lower insurance premiums. Georgetown took the savings and increased its business continuity insurance fivefold. "When Hurricane Katrina hit, many of the affected universities had just a fraction of the insurance we had, and it wasn't enough," says Dimolitsas. "When we began raising debt in the market, we discovered that underwriters, concerned about vulnerabilities, liked that the school was so well protected. That was another financial benefit."

Dimolitsas also had an advantage that many of his peers at other organizations don't: management that, spurred by a series of traumatic events, wanted to take action. Most enterprises have never been affected by terrorist attacks, earthquakes, or pandemics. There is little incentive to spend the time and money to combat

Why You Are at Risk

It's not just hackers and competitors you need to worry about. Many of the risks businesses face are subtle or indirect. Here are a few things to watch out for:

- Supply chains and markets have gone global. That means there are a whole new set of potential crises—natural disasters, political unrest, cultural clashes—you need to worry about and plan for.
- Outsourcing can reduce costs, but it also reduces control. If your partner suffers a fire or a labor strike, it's your problem too.
- Using a single source for goods may get you a better price, but it also means there is no easy alternative if your supplier suddenly shuts down.
- A tsunami may not hit you, but a terrorist attack might. By themselves, most disruptions are a one-in-a-million event. But taken together, the odds add up. Instead of downplaying all the crises that probably won't strike, think about the damage caused if any one of them does. And prepare for that.
- Employees leave. Their knowledge may not wind up at a competitor, but it still may be lost. Do you have a system in place to capture and share all the tacit know-how your veteran staffers have developed over the years?

incidents that haven't yet happened. So perhaps the best way to provide the incentive isn't to look to the future but at the present. "The idea is to give executives situational awareness of their levels of resiliency, to motivate them to action," says Darryl Moody, COO of Resilient Corp., a business intelligence provider in Washington, D.C. "If something can be measured, it can be managed."

To that end, Resilient has developed what it calls its Resiliency Posture Index. It establishes objective performance measures: scores for ten key areas within an enterprise, including information security, supply-chain management, public relations, disaster management, human capital, legal and regulatory, and corporate strategy. The scores (from 0 to 4) don't tell an enterprise whether it is resilient, but rather gauges the likelihood that it is. "We'll deploy a team to the company, with experts in each of these areas," says Moody. "We'll collect information about how they do these functions from interviews, surveys, and third-party sources."

Each of the categories is broken down into dozens of activities; for example, for information security, Resilient Corporation will look at the procedures in place to secure data, at the IT department's management, at corporate policies and governance, and so on. All of this is analyzed and rated and compared with industry averages. "The idea is to give executives measurements so they can decide if they need to do something more," says Moody. "If they have a 4.0, they know they're at a world-class level. If they get a 2 when their industry averages a 3.8, they know they need to do something." The scores also provide companies a baseline for the next time they're assessed. "That lets them see if the measures they are putting into place are working," says Moody.

Taking Tactical Measures

Fortunately, an enterprise can take some basic first steps to become more resilient. "It's important to think less about the cause and more about the impact of a major disruptive event," says James H. Quigley, chief executive officer of Deloitte & Touche USA LLP, whose subsidiary firms provide consulting and advisory services for organizations across the globe. "A terror attack, a hurricane, and a transit strike are three completely different threats, but they can have one similar outcome: they prevent people from getting to work. "When you think about the outcome, rather than the cause, you can achieve a better result and less disruption."

Next, says Quigley, comes a framework—principles and processes for assessing and managing risk. "You would be surprised at how many companies lack this foundation. Think, for example, about delegation of authority—the ability of any one individual to 'bet the farm.' We've seen a couple of massive trading losses in recent years because, incredibly, the companies did not have controls over how much capital any one trader could put at risk." Sound communication is important, too. "Executives must let the entire organization know that risk management is everybody's job," says Quigley. "You spread the message through many communications channels. You do it through training and workshops. And you don't brand those who tell you something could go wrong as 'negative thinkers.' Instead, you encourage opinions and dissent in ways that allow for reasonable concerns to be evaluated and addressed."

It's also crucial is to consider the resiliency of all the partners and suppliers with whom you work. The cliché holds true: You're only as strong as your weakest

link. During the 9/11 terrorist attacks, systems at the NASDAQ stock market—which had spent the previous 20 years honing its backup, emergency operations, and contingency plans—remained operational throughout the day. But its customers' systems, which had to connect to NASDAQ electronically, did not, so trading was interrupted. "The Wall Street firms did, in fact, have backup centers, but in many, many cases these were not designed or tested for actual use," says Anna Ewing, executive vice president of operations and technology and chief information officer of The Nasdaq Stock Market Inc. "They were using outdated software or had connectivity problems. They'd have multiple data centers but put them all within ten blocks, while we had ours 300 miles apart. The big lesson from 9/11 was that operational readiness must exist in a practical sense—not just on paper or in the form of backup centers that were essentially gathering dust."

Many companies perceive risk management as a cost center and relegate the issue to the back office.

At NASDAQ, it became clear that tests and simulations involving its own systems were not enough; all of its partners had to be included. And these tests had to be performed on a regular basis. "We increased testing of our backup sites from every quarter to every month," says Ewing. "And now we incorporate not only customers but also key service providers. For any industry, the supply chain is critical for the business to operate."

Indeed, the key to resiliency is to think of it as a moving target. Processes should never be implemented and left alone, but constantly examined and refined. During Hurricane Katrina, Wal-Mart reopened 70 affected locations within 48 hours and delivered essential supplies, such as water and generators, when even the federal government saw its supply lines snagged. This wasn't the result of some grand plan developed back in the corporate war room. It was the result of years of handling emergencies and learning how to handle the next one better.

"It's a constant process," says Jason Jackson, Wal-Mart's director of emergency management. "We'll look at risk and annually revise our business continuity plans." Each evaluation incorporates new lessons and generates new ideas. "In 2004 we had four pretty good-sized hurricanes hit us within six weeks, and we learned that people can't go 18 to 20 hours a day for that long in our emergency operations center," says Jackson. "So we added more depth in each department. We had that in place in 2005 when Katrina hit. And in 2006 we geared up with even more bench support."

Technology can also play a big role in resiliency. In Wal-Mart's emergency command post in Arkansas, staffers track news, e-mail, and web feeds from the National Weather Service, the U.S. Geological Survey, the Department of Homeland Security, and the Centers for Disease Control, among other sources. Distribution lists have been created so that once a crisis and its scope have been identified, appropriate managers can be contacted. A high-tech alert service, called Send Word Now, delivers instantaneous voice and text messages.

Yet Wal-Mart learned that you have to strike a balance between the old and new ways of communicating. "BlackBerries and Treos are great, but face-to-face communication is absolutely critical," says Jackson. "By putting managers from all of our departments in one room, we can see their emotions and make sure that everyone has the same information. During Katrina, the operations manager would get a call that New Orleans needed ten trailers of water. He would turn to the replenishment manager, who would go to the logistics manager, who would get the water there."

Resiliency requires patience and planning. It won't happen overnight. But once you've achieved it, neither will your downfall. ■