

Anticipating Disaster, or Putting the Fear of God into Top Management

JOSEPH COATES

ACTS OF GOD ARE THE MOST WIDESPREAD and disastrous events to plague us on Planet Earth. Second, but less common and often more regional, are the acts of one or more devils-as terrorists, psychos or vengeful individuals. Third, and more common and usually less destructive, are the individual acts of incompetents—all too often committed in technological systems.

Katrina illustrates the first, 9/11 the second, and Bhopal, Chernobyl and most regional blackouts illustrate the third.

In complex systems—the only systems worth worrying about—the three types may be all involved, as the auto companies, for years, tried to blame not faulty design but the “nut behind the wheel” for most deadly auto accidents. Human beings are rarely the totally responsible source of an industrial accident, even when it is Category Two above. In our complex technological world, people and machines are components of a single system, in which good design can severely limit or eliminate the risk of failure, misbehavior, faults, or difficulties with any or all components.

Why must we continually experience disasters and catastrophes? Limiting the answer only to the United States, the primary reasons lie in the reality that American business optimizes on the short run, and therefore generally has no interest in anticipating low-probability, high-severity outcomes. We find consistently, in our futures studies, that when we identify “wild cards” of mid-to-low probability affecting any mid-to-large-size business, the inventory can easily run from 50 to 125 incidents. These large numbers usually surprise our clients, because they have never assayed them, nor paid attention to others’ analyses of wild cards.

Kinds of Wild Cards

Generally the wild cards fall into two categories: First, acts of God—that is, meteorological or

geophysical events; second are socioeconomic events such as a sharp increase in credit card defaults or a pandemic. “Ho-hum” usually succeeds a flash of concern unless there is an unequivocal crippling implication, or a way to cheaply undercut the risk with safeguards, or there are clear, workable, low-cost routes to recovery.

Both government and corporations cut corners, especially when the cut corners are literally invisible to most observers. Corner-cutting is the usual response to budget cutting, which in the case of government is well documented as the result of technologically uninformed legislators making arbitrary decisions about projects. Those in the agencies with engineering responsibility are often timid or intimidated about driving home the riskiness of legislative penury. Consider, with regard to Katrina, the Congress and the Corps of Engineers, as they got down to the levee.

Waking Up the Corporation

What will make corporations more aware and more responsible for their component of anticipatable technological disasters or catastrophes? First are incidents in their own industry. There is severely limited psychological capability to transfer the sensitivity to risk from someone else’s sector to your own. Linked to this, of course, is the need for an aggressive assignment, internally or through consultants, to analyze the susceptibility of a company’s systems to any of the three types of disasters noted above.

Second will be lawsuits, most likely the class action kind, reflecting failure to identify risks or the failure to adequately deal with risks when identified by the industry or in one’s own company. Just consider what class actions have done to the tobacco and asbestos industries.

Corporate boards may act but only when it is clear that they have a fiduciary responsibility, which the failure to exercise will land them broke and in the pokey.

Whistle-blowers within the company have potentially powerful leverage, but they cannot be counted on to be there.

Trade associations and industrial research organizations may incur crippling liability from failure to explore and to act on identified risks.

In this period of a dramatically pro-business White House, it is unlikely that it will put forward a serious risk initiative. See for example the recent (October 2005) legislation protecting the firearms industry from a broad range of suits, protection which the President had promised to sign before the bill was passed.

An unusual degree of foresight on the part of CEOs, chairmen or Boards is possible in individual cases, but foolish to believe in as a general expectation.

In specific businesses or systems, the risks to workers may be so high as to initiate a union or other organized campaign for risk management. Similarly, in communities in which the risk to the community is high, local pressure may force corporate action by lawsuit or through regulation.

R&D managers may on their own hook explore the full range of technological and physical risks and the means of coping with them, to put before top management.

Job for CTO/R&D Director

I wouldn't bank on any of the above. But I would place the highest confidence of a significant useful outcome in an assay of technological risks and mitigation mechanisms by the chief technology officer or the director of R&D or whoever else is the technological top dog. In all likelihood, however, they would have to be given the assignment by top management for the following reason:

An analysis of the risks and mitigating actions is likely to be laden with uncongenial news and unfamiliar choices. Therefore, to assure a comprehensive no-holds-barred analysis, most of the people who could do the job would have to have top management's support before they begin.

A technology that is likely to fail, either because of a systems difficulty or a geophysical event, is best understood by a technology executive.

He or she also has the best likelihood of being able to interpret information from the press, government, association reports, or scientific and technical journals about the implications for his or her company.

A Process To Follow

While there is no clear fixed route to understanding, the following process is universally valid.

First, assess the geophysical situation of the firm's different facilities, e.g., in an earthquake zone, in avalanche territory, in a hurricane or tornado region, volcanic activity, heavy snowfall, on river floodplains, or some other place with a history of geophysical destruction. For example, how many people are aware of the fact that the most severe earthquake in the U.S. was outside St. Louis, Missouri, and was felt from Montana to South Carolina? It even made the Mississippi River flow backward.

Each geophysical risk should be studied for frequency and severity in order to evaluate the choices for prevention and recovery. Sometimes there may be an intervening step such as a geophysical event knocking out electric power source scores or hundreds of miles away. Tied to each risk must be a hard-nosed evaluation of how much warning could one expect, from whom, and why, since in many cases one could mitigate the risk by a well-ordered shutdown.

The risks from individuals, either working alone or in some organized manner, (e.g., terrorist activity) are in many regards more dangerous and more difficult to anticipate, since they require the analyst to put him or herself into the shoes of the would-be bad actor. That single bad actor (e.g., disgruntled employee) is likely to have detailed, specific knowledge of a few critical places whose elimination could have disastrous effects.

Terrorists acting in concert are likely to bring more destructive resources to bear, and to act with no warning, at one or more sites within a facility in order to maximize destruction and/or loss of life.

Some kinds of facilities are more subject to destruction than others, and some facilities carry the substantially higher risk of killing or maiming workers and neighbors. The highest on my list are chemical companies in metropolitan areas and/or in proximity to other hazardous facilities. Hence the need for cooperation among those who have similar or related facilities at risk.

The problem of notifying the community is extremely important but as far as we know virtually neglected, and evacuation is unpracticed.

The risks from accidents should be thoroughly explored as well, because users' behavior and habits may be radically different from the designer's assumptions, e.g., a valve may close to the left rather than to the right.

Local resources—police, fire, National Guard, close-by military bases—are all potential resources for dealing with an event. At the low end of susceptibility to disastrous sabotage or incidents are heavy manufacturing facilities, steel mills and similar hardened sites.

Plans: How Useful?

For every risk there must be a plan, which itself will be totally useless unless it is practiced. Solid research shows that emergency plans are ignored unless they have actually been exercised.

An incidental but important public relations step is to have a pre-designated top executive who will be the company's only voice in a disaster. He or she must be selected with the greatest care and also rehearsed in the function of corporate mouthpiece.

There is of course a vast literature on hazards, risks and disasters, which can be drawn upon for both generic and specific understanding of prevention and recovery. Discussion with Homeland Security, the appropriate state officials, and the equivalent in the local jurisdiction are certainly in order.

For those readers who would like to see an inventory and description of man-made catastrophes, Lee Davis's 400-page treatment of hundreds of them in *Man-Made Catastrophes*, Checkmark Books, New York, N.Y., may whet their appetite.