BOOKS: TECHNOLOGY

Learning Limits from Failures

Lloyd J. Dumas

The extraordinary, accelerating advance of science and technology over the past few hundred years has been intoxicating. It fills us with a sense of nearly unlimited possibility for understanding and manipulating the physical world to enhance the well-being of humans. But although science and technology have made us more powerful than ever, there is no reason to suspect that we are now any less fallible than before, and there lies the rub. For at the interface between our growing technological power and our unchanging proneness to err lies the potential for increasing disaster. In *Inviting Disaster: Lessons from the Edge of Technology*, James R. Chiles takes us inside many notable technological accidents for a detailed look at the sequence of events and missteps that can turn what began as an ordinary experience into a "really bad day."

Inviting Disaster
Lessons from the Edge of Technology
by James R. Chiles
HarperBusiness, New York, 2001. 352 pp. $28, C$42.50. ISBN 0-06-662081-3.

Technology writer Chiles argues that "in our new world surrounded by machines occasionally gone savage, we need to acknowledge the extraordinary damage that ordinary mistakes can now cause...." That is certainly true. The difference between a trivial error and a catastrophic error often lies not in the error itself, but in its context. Entering the wrong sequence of numbers while making a telephone call means the switching computer will ring the wrong phone, an annoying but trivial mistake. However, one night in December 1995, the pilots of American Airlines Flight 965 made essentially the same mistake as they flew toward Cali, Colombia. They entered the wrong sequence into a computer, their navigational computer. The plane steered into a mountain, and 160 people died.

Chiles emphasizes the step-wise character of many disasters. Though they may seem to arise suddenly, "disasters nearly always require multiple failures and mistakes to reach fruition." He observes that a "disaster occurs through a combination of poor maintenance, bad communication, and shortcuts." I would add hidden or apparently minor design errors to that list. The explosion of the space shuttle Challenger, the partial meltdown at the Three Mile Island nuclear power plant, and the sinkings of the "unsinkable" offshore drilling platform *Ocean Ranger* and the *Titanic* are examples of what Chiles calls "systems fractures," in an analogy to how metal cracks under stress. He tells the intriguing stories of these and other technological disasters in varying detail, from a chapter-long recounting of the *Ocean Ranger*'s demise to scattered paragraphs on the *Titanic*.

Disaster at the human-machine interface rarely has one cause, but there is often a linchpin problem. Sometimes it is a technical "blind spot," such as the lack of coolant-level indicators that prevented Three Mile Island's operators from realizing coolant levels were actually becoming dangerously low, not growing too high as they had suspected. Sometimes the crucial problem is the pressure to get the job done quickly, such as pressures to meet scheduled launches that helped do in the Challenger and, 56 years earlier, the British airship *R.101*. Sometimes the problem is "people so tightly focused on a goal, so consumed with the job ahead, that they refuse to heed information coming from outside," the failure that played a key role in the fatal Apollo 1 fire and the crash of a ValuJet flight into the Everglades.

Normal human physical limitations, such as susceptibility to fatigue and circadian disruption, magnify error and often prevent the clear thinking and quick action required to stop a spreading system "crack" before it becomes a system fracture. Critical events leading to the deadly chemical release from Union Carbide's Bhopal plant, the Chernobyl disaster, and Three Mile Island all happened in the early morning. Stress-induced psychological limitations, such as "cognitive lock" and "hypervigilance," can also interfere with effective action. Cognitive lock occurs when those dealing with a crisis latch on to a fixed mental picture of what is happening and the course of action that picture implies, treating contradictory evidence as a time-wasting distraction. In a state of hypervigilance, accompanied by hyperventilation and peak heart rates, people cannot think clearly or remember their training.

The growing human-technological–failure literature ranges from gee-whiz storytelling to more serious analytic work, such as Charles Perrow's classic *Normal Accidents* (*1*), Scott Sagan's *Limits of Safety* (*2*), and (I hope) my own, *Lethal Arrogance* (*3*). Heavily weighted toward stories and relatively light on analysis, *Inviting Disaster* falls into the middle of that range.

What conclusions are we to draw? Chiles notes that "[e]ven the best-run systems always have something off-line or running out-of-tolerance...No force on earth can get everything to stay in balance all the time." He recognizes that we have to live with imperfect systems, and he suggests that this means there are certain technologies that we have a responsibility not to accept. With flexible fault-tolerant systems, vigilant workers, and a management devoted to safety, "problems can be stopped short of disaster—most of the time." But most of the time is not all of the time, and there are cases where all of the time is the only thing we can live with. Chiles argues that "where the consequences are irreversible and final, such as an accidental nuclear war...I find it hard to believe that we'll be able to keep our collective finger on this hair trigger indefinitely without twitching even once."

Chain-reaction catastrophe. The July 2000 Concorde crash at Paris began with a small piece of debris on a runway, which led to the blow out of a tire, the rupture of a wing tank, the streaming of fuel into an engine intake, and the loss of control of the plane.

There is thus a crucial dichotomy. For most technologies, the answer is to learn from mistakes, do the best we can, and face up to our inability to eliminate risk. But for a few of the most dangerous ones—such as systems capable of producing mass destruction—even a tiny risk is intolerably high. For those technologies, we must insist on perfection. Chiles comments, "To insist on perfection is to shut the whole thing off." To which I reply, "Amen."

References
1. C. Perrow, *Normal Accidents: Living with High-Risk Technologies* (Basic Books, New York, 1984).
2. S. D. Sagan, *Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton Univ. Press, Princeton, NJ, 1993).
3. L. J. Dumas, *Lethal Arrogance: Human Fallibility and Dangerous Technologies* (St. Martin's, New York, 1999).

The author is in the School of Social Sciences, University of Texas at Dallas, Richardson, TX 75083–0688, USA. E-mail: ljdumas@utdallas.edu