Computer-Related Risks

**by Peter G. Neumann**
**ACM Press/Addison-Wesley**
**367 pages, $24.95**
**ISBN# 0-201-55805-X**

# Computer-Related Risks

When most of us think of "risks," we think of crossing the street, driving down the road or venturing into a rough neighborhood. "Computer-related risks" conjures up visions of viruses and malicious hackers; these are relevant images, but the concept is actually deeper and broader than many people perceive.

Computer-related risks are just that: unanticipated behavior in a system that in some way makes use of a computer, with results that can potentially disrupt operations or harm people or property. A risk can produce a safety problem; a monetary loss; a security vulnerability; a loss of privacy; an unexpected interruption in some kind of service; a loss of life; a power failure; or simply an irritation. Sabotage by resentful employees as well as errors by confused but well-intentioned users probably do more damage than hackers and viruses, yet few of us would thinks of these as "risks." On the other hand, two different roller coaster crashes that injured a total of 42 people were considered computer-related, because the failures were in a sensor-based monitoring system. Although attributed to human factors, the Chernobyl nuclear plant disaster was also computer-related, because the relative complexity of the plant's systems made it more difficult for the staff to control.

By Jim Johnson

The use of autopiloting systems by airlines and rail systems is meant to reduce passenger risk, but some recent, well-publicized tragedies have revealed that such systems introduce new risks of their own, and many organizations are reassessing what constitutes appropriate use of these systems. Most of us would consider bugs in computer date programs to be at worst an irritant, but leap years, time-zone shifts and errors in calibration sequences have crashed entire ATM systems, damaged a steel factory in Germany when molten steel wasn't given adequate time to cool and, in one incident in Colorado that resulted in a death, caused computer-controlled street-crossing systems to malfunction.

Builders of complex information systems for government and industry engage in some form of risk management and factor unforeseen problems into their designs and projections. Yet deadlines, unexpected events and system failures impact even the best plans. All too often, hindsight reveals that these mishaps could have been predicted, avoided or at least managed more effectively. The explosion of the space shuttle Challenger, for example, was initially ascribed to a failed O-ring, but subsequent investigations also revealed instances of disregarded warnings from engineers. We could say that the January 1990 blockage of approximately five million calls over AT&T's telephone network was caused by an obscure bug in some C code, but compilers could also be faulted in failing to flag the error; as could testing procedures that were extensive but nonetheless inadequate.

Peter Neumann, principal scientist at the computer science lab of SRI International in Palo Alto, CA, knows about computer-related risks. In 1985 he started the popular online Risks Forum, which is gatewayed to the comp.risks Usenet newsgroup. He's also a fellow of the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers, and writes the "Inside Risks" column for *Communications of the ACM.*

In the preface to *Computer-Related Risks*, Neumann makes it clear that he intends to target several distinct audiences. This multifaceted approach has produced a book with several personalities, the most illustrative (and most entertaining) of which is a relentless recitation of technology-related incidents and anecdotes from recent history. Neumann's eye for irony and frequent use of puns, combined with the alternately hilarious and horrifying accounts of mishaps and disasters, make this the kind of book that will make you want to stay up late reading. Also, the seemingly endless accounts of disasters and near-disasters resulting from ignored procedures, human error and obscure software bugs is enough to give anyone the willies about our civilization's dance along the technological bleeding edge.

## Fun and Useful

As entertaining as this book may be, its application of humor and spectacle doesn't detract from the analytical usefulness. Solid reasoning and occasional forays into dense technical jargon remind the reader that Neumann is, first and foremost, a scientist. Each chapter's case histories are graphed according to source of risk, illustrating which kinds of risks have more predictable causes and which are more varied in origin. Chapter summaries facilitate skimming and review, and the end of each chapter offers a list of textbook-style "challenges" that invite the reader to analyze the cases presented and devise strategies for crisis prevention and risk management. Together, these attributes assert the book's usefulness as a text in institutions of higher learning, as well as a tool for management evaluation and professional development.

Chapter 1 is a general introduction to the topic, offering an overview of the nature of risks. In chapters 2 through 6, Neumann groups his cases according to their specific attributes: reliability, safety, security, privacy and well-being. Chapter 7 is devoted to risk reduction and the overall systems view of risks; chapter 8 covers the more human side; and chapter 9 offers conclusions and comments about the implications of our increasing dependence on incredibly complex technology. A glossary is provided for nonengineers; a lengthy index, a bibliography, an appendix on background materials, notes and references top it off.

Some nontechnical readers may get befuddled when Neumann occasionally lapses into geek-speak, but skipping over these parts doesn't harm one's comprehension of the material, and engineers are sure to benefit from it. Likewise, Neumann's precise terminology and categorization of risk attributes (differentiating between "risk," "threat" and "vulnerability," for example) may seem like hair-splitting to some, but general readers can easily and safely ignore these references, which will appeal to those seeking a more exacting approach.

## Emphasis on Analysis

Although suggested procedures for minimizing risks are provided, a significantly greater number of pages is devoted to the case briefs; there is a greater emphasis on analysis of risks than on their prevention. The book is more of an exploration of events and concepts than a guide to how to play it safe. This might be due to the author's strongly held belief that our technological world cannot be made a safe place and that we'd better accept the idea. Neumann writes, "No system can ever be guaranteed to work acceptably all of the time. In a complex system, it is essentially impossible to predict all the sources of catastrophic failure. This caveat is true even in well-engineered systems, where the sources of failure may be subtle."

His emphasis on analysis is more a function of the nature of risk itself than a personal attitude on the part of the author, and he's certainly no Luddite. Since a broad, cross-industry, how-to-be-safe methodology simply doesn't exist, there isn't a viable alternative to conducting a comprehensive risk analysis specific to one's own situation; to believe otherwise would only increase the likelihood of disaster. Managers and executives should hear the ring of truth in his conclusions and recommendations; among other things, Neumann points the finger at wishful thinking and corner-cutting in the design of systems and procedures. In asserting the concept of "defensive design," he also takes upper-echelon scapegoating to task: "It is self-defeating to pin the blame on a donkey—for example, on a designer, programmer, system operator or penetrator, or worse yet, *on the computer*. Blame is often simplistically misplaced. Several factors may be involved. Especially in distributed systems, blame is typically distributed."

Neumann's recommendations for minimizing risks are thorough and sound, if not quite as much fun as the other sections of the book. His discussion of methods useful to managers, executives and staffers alike makes this book an important read for everyone involved in the production of complex systems. We all know customers, managers and marketers who don't want to hear this expert's assertion that "guaranteed system behavior is impossible to achieve," but he deserves kudos for being a credentialed person who is willing to tell it like it is. IT

***Jim Johnson** is a certified personnel consultant and the principal of Options Unlimited, specializing in the placement of Unix professionals in the Washington, DC, area. He can be reached at jim@uujobs.com.*

*To purchase books in this column, contact your local bookseller.*