NOTES

[1] *The Risks Digest: Forum on Risks to the Public In Computers and Related Systems* (formerly the comp.risks newsgroup on Usenet). Archived at catless.ncl.ac.uk/Risks; current issue at www.csl.sri.com/~risko/risks.txt.

[2] Philip E. Ross, "The Day the Software Crashed," *Forbes*, April 25, 1994, 153:9, pp. 142–156. Peter G. Neumann, "Inside Risks," *Communications of the ACM*, July 1992, p. 122.

[3] Jeffrey Rothfeder, *Privacy For Sale*, Simon & Schuster, 1992, p. 34 and pp. 130–131; "A Case of Mistaken Identity," *Privacy Journal*, Dec. 1992, p. 7; "In the States," *Privacy Journal*, Jan. 1993, p. 3; Neumann, "Inside Risks," *Communications of the ACM*, Jan. 1992, p. 186, and July 1992, p. 122. "Reading Privacy Journal's Mail," *Privacy Journal*, Aug. 1998, pp. 1, 3, 5.

[4] Andrea Robinson, "Firm: State Told Felon Voter List May Cause Errors," *Miami Herald*, Feb. 17, 2001.

[5] Paul M. Barrett, "Aiding Prosecutions, Justices Allow Use Of Some Improperly Obtained Evidence," *Wall Street Journal*, March 2, 1995, p. B4.

[6] *Arizona v. Evans*, reported in "Supreme Court Rules on Use of Inaccurate Computer Records," *EPIC Alert*, March 9, 1995, v. 2.04.

[7] Associated Press, "Teen 'Convicted' by Computer," *San Jose Mercury*, Mar. 7, 1996, p. 3B.

[8] Dan Joyce, e-mail correspondence, May 17, 1996 (the adoption case). Study by the Office of Technology Assessment, reported in Rothfeder, *Privacy For Sale*. "Jailing the Wrong Man," *Time*, Feb. 25, 1985, p. 25. David Burnham, "Tales of a Computer State," *The Nation*, April 1983, p. 527. Evelyn Richards, "Proposed FBI Crime Computer System Raises Questions on Accuracy, Privacy," *Washington Post*, Feb. 13, 1989, p. A6. "Wrong Suspect Settles His Case of $55,000," *New York Times*, Mar. 6, 1998, p. 30. Peter G. Neumann, "Risks to the Public in Computer and Related Systems," *Software Engineering Notes*, Apr. 1988, 13:2, p. 11. Several similar cases are reported by Peter G. Neumann in "Inside Risks," *Communications of the ACM*, Jan. 1992, p. 186.

[9] *Privacy Journal*, Aug. 1998, p. 4.

[10] "AT&T Crash, 15 Jan 90: The Official Report," in "Subsection on Telephone Systems," *Software Engineering Notes*, April 1990, 15:2, p. 11–14. Ross, "The Day the Software Crashed." Ann Lindstrom, "Outage Hits AT&T in New England," *Telephony*, Nov. 11, 1991, 221:20, p. 10. "Bell Atlantic Customers Put on Hold by Directory Assistance," Nov. 26, 1996, PGN Abstracting.

[11] Penni Crabtree, "AT&T system crash is wake-up call for business," *San Diego Union–Tribune*, Apr. 15, 1998, p. C1. "Data Entry Typo Mutes Millions of U.S. Pagers," *Wall Street Journal*, Sep. 27, 1995, p. A11.

[12] Frederic M. Biddle, John Lippman, and Stephanie N. Mehta, "One Satellite Fails, and the World Goes Awry," *Wall Street Journal*, May 21, 1998, p. B1.

[13] David Craig, "NASDAQ Blackout Rattles Investors," *USA Today*, July 18, 1994, p. 2B. Associated Press, "NASDAQ Defends Its System after Stock-Pricing Errors," *New York Times*, Sept. 13, 1994, p. D19. "Note to Readers," *Boston Globe*, Oct. 25, 1994, p. 52. Julia Flynn, Sara Calian, and Michael R. Sesit, "Computer Snag Halts London Market 8 Hours," *Wall Street Journal*, Apr. 6, 2000, p. A14.

[14] Thomas Hoffman, "NCR Users Cry Foul Over I Series Glitch," *Computerworld*, Feb. 15, 1993, p. 72. Milo Geyelin, "Faulty Software Means Business for Litigators," *Wall Street Journal*, Jan. 21, 1994, p. B1. Milo Geyelin, "How an NCR System for Inventory Control Turned into a Virtual Saboteur," *Wall Street Journal*, Aug. 8, 1994, p. A1, A5. Mary Brandel and Thomas Hoffman, "User Lawsuits Drag On for NCR," *Computerworld*, Aug. 15, 1994, p. 1.

[15] Jacques Steinberg and Diana B. Henriques, "When a Test Fails the Schools, Careers and Reputations Suffer," *New York Times*, May 21, 2001, pp. A1, A10–A11.

[16] The DIA delay was widely reported in the news media. A few of the articles used as sources for the discussion here are W. Wayt Gibbs, "Software's Chronic Crisis," *Scientific American*, Sept. 1994, 271:3, pp. 86–95. Robert L. Scheier, "Software Snafu Grounds Denver's High-tech Airport," *PC Week*, 11:19, May 16, 1994, p. 1. Price Colman, "Software Glitch Could Be the Hitch. Misplaced Comma Might Dull Baggage System's Cutting Edge," *Rocky Mountain News*, April 30, 1994, p. 9A. Steve Higgins, "Denver Airport: Another Tale of Government High-Tech Run Amok" *Investor's Business Daily*, May 23, 1994, p. A4. Julie Schmit, "Tiny Company Is Blamed for Denver Delays," *USA Today*, May 5, 1994, pp. 1B, 2B.

[17] Scheier, "Software Snafu Grounds Denver's High-tech Airport."

[18] Carl Ingram, "DMV Spent $44 Million on Failed Project," *Los Angeles Times*, April 27, 1994, p. A3. Effy Oz, "When Professional Standards Are Lax: The CONFIRM Failure and its Lessons," *Communications of the ACM*, Oct. 1994, 37:10, pp. 29–36. Virginia Ellis, "Snarled Child Support Computer Project Dies," *Los Angeles Times*, Nov. 21, 1997, p. A1, A28. Peter G. Neumann, "System Development Woes,", *Communications of the ACM*, Dec. 1997, p. 160.

[19] Data compiled by Peter Mellor, Centre for Software Reliability, England, reprinted in Peter G. Neumann, *Computer-Related Risks*, Addison Wesley, 1995, p. 309.

[20] "Airbus Safety Claim 'Cannot Be Proved'," *New Scientist*, Sept. 7, 1991, 131:1785, p. 30. Robert Morrell

Jr., *Risks Forum Digest*, July 6, 1994, 16:20. "Training 'Inadequate' Says A320 Crash Report," *Flight International*, Dec. 22, 1993, p. 11 (on the Jan. 1992 Strasbourg A320 crash, excerpted by Peter B. Ladkin in *Risks Forum Digest*, Jan. 2, 1994). Ross, "The Day the Software Crashed," p. 156, on the 1993 Warsaw crash. David Learmont, "Lessons from the Cockpit," *Flight International*, Jan. 11, 1994.

[21] William M. Carley, "New Cockpit Systems Broaden the Margin of Safety for Pilots," *Wall Street Journal*, Mar. 1, 2000, pp. A1, A10. Barry H. Kantowitz, "Pilot Workload and Flightdeck Automation," in M. Mouloua and R. Parasuraman, eds., *Human Performance in Automated Systems: Current Research and Trends*, pp. 212–223 (TCAS problems on p. 214).

[22] Alan Levin, "FAA finally unveils new radar system," *USA Today*, Jan. 20, 1999, p. 01.A. Anna Wilde Mathews and Susan Carey, "Airports have delays, cancellations due to problems in air-traffic control," *Wall Street Journal*, May 7, 1999, p. A20. "Software Glitch" (editorial), *San Diego Union–Tribune*, Oct. 23, 2000, p. B8. Robert Fox, "News Track: Air Communication Breakdown," *Communications of the ACM*, Aug. 2000, 43:8, p. 10.

[23] Nancy G. Leveson and Clark S. Turner, "An Investigation of the Therac-25 Accidents," *IEEE Computer*, July 1993, 26:7, pp. 18–41. Jonathan Jacky, "Safety-Critical Computing: Hazards, Practices, Standards, and Regulation," in Charles Dunlop and Rob Kling, eds., *Computerization and Controversy*, Academic Press, 1991, pp. 612–631. Most of the factual information about the Therac-25 incidents in this chapter is from Leveson and Turner.

[24] Conversation with Nancy Leveson, Jan. 19, 1995.

[25] Jonathan Jacky, "Safety-Critical Computing," p. 615. Peter G. Neumann, "Risks to the Public in Computers and Related Systems," *Software Engineering Notes*, April 1991, 16:2, p. 4. Ted Wendling, "Lethal Doses: Radiation That Kills," *Cleveland Plain Dealer*, Dec. 16, 1992, p. 12A. (I thank my student Irene Radomyshelsky for bringing the last reference to my attention.)

[26] W. W. Norton, 1997, p. 157.

[27] "Airbus Safety Claim 'Cannot Be Proved'," p. 30.

[28] Richard P. Feynman, *What Do You Care What Other People Think?*, W. W. Norton & Co., 1988.

[29] The report of the inquiry into the explosion is at www.esrin.esa.it/htdocs/tidc/Press/Press96/ariane5rep.html.

[30] From an e-mail advertisement for Nancy G. Leveson, *Safeware: System Safety and Computers*, Addison Wesley, 1995.

[31] A particularly good article discussing human factors and the causes of the crash is Stephen Manes, "A Fatal Outcome From Misplaced Trust in 'Data'," *New York Times*, Sept. 17, 1996, p. B11.

[32] Kantowitz, "Pilot Workload and Flightdeck Automation."

[33] Feynman, *What Do You Care What Other People Think?* The shuttle was not immune to problems. The Risks Forum includes reports of computer failures caused by a loose piece of solder, subtle timing errors, and other factors.

[34] "AT&T Crash, 15 Jan 90: The Official Report."

[35] Feynman, *What Do You Care What Other People Think?*, pp. 190–194 and 232–236. Aeronautics and Space Engineering Board, National Research Council, *An Assessment of Space Shuttle Flight Software Development Processes*, National Academy Press, 1993.

[36] Mary Brandel and Thomas Hoffman, "User Lawsuits Drag On for NCR," *Computerworld*, Aug. 15, 1994, p. 1.

[37] This issue is raised by Professor Philip Koopman of Carnegie Mellon University. See his Web site, www-2.cs.cmu.edu/~koopman/ucita/ for more on UCITA.

[38] These problems and trade-offs occur often with regulation of new drugs and medical devices, regulation of pollution, and various kinds of safety regulation. They are discussed primarily in journals on the economics of regulation.

[39] Jacky, "Safety-Critical Computing," p. 624.

[40] Leveson and Turner, "An Investigation of the Therac-25 Accidents," p. 40.

[41] See, for example, Walter Williams, *The State Against Blacks*, McGraw-Hill, 1982, Chapters 5–7. One year during a construction lull, a state failed everyone who took the building contractor's license exam. It is illegal in 48 states for most software engineers to call themselves software engineers because of licensing laws for engineers. One company was forced to spend thousands of dollars changing job titles, business cards, and marketing literature to remove the word "engineer." (Julia King, "Engineers to IS: Drop That Title!" *Computerworld*, May 30, 1994, 28:22, pp. 1, 119.)

[42] "More Risks of Computer Billing—$22,000 Water Bill," *Software Engineering Notes*, Oct. 1991, 16:4, p. 6. Richard M. Rosenberg, "Success Components for the 21st Century," *The Magazine of Bank Management*, Jan/Feb. 1994.

[43] Raju Narisetti, Thomas E. Weber, and Rebecca Quick, "How Computers Calmly Handled Stock Frenzy," *Wall Street Journal*, Oct. 30, 1997, p. B1, B7. Peter G. Neumann, "System Development Woes," *Communications of the ACM*, Dec. 1997, p. 160.

[44] William M. Carley, "New Cockpit Systems Broaden the Margin of Safety for Pilots," *Wall Street Journal*, Mar. 1, 2000, p. A1.

[45] Holman W. Jenkins Jr., "Look Ma, No Hands!" *Wall Street Journal*, Oct. 20, 1999, p. A27. William M. Carley, "Could a Minor Change in Design Have Saved American Flight 965?" *Wall Street Journal*, Jan. 8, 1995, pp. A1, A8. National Air Transportation Safety Board and the U. S. Bureau of the Census, *Statistical Abstract of the United States: 1994*, Tables 134

and 996. Air Transport Association, reported in "Safer Skies," *Wall Street Journal*, July 9, 1999, p. W4.

46 Miles Corwin and John L. Mitchell, "Fire Disrupts L.A. Phones, Services," *Los Angeles Times*, March 16, 1994, p. A1.

47 Heather Bryant, an Albertson's manager, quoted in Penni Crabtree, "Glitch fouls up nation's business," *San Diego Union–Tribune*, Apr. 14, 1998, p. C1.

48 An excellent "Nova" series, "Escape! Because Accidents Happen," aired Feb. 16 and 17, 1999, shows examples from 2000 years of history of inventing ways to reduce the injuries and deaths from fires and from boat, car, and airplane accidents.

49 "A Fistful of Risks," *Discover*, May 1996, p. 82.

50 Tom Forester and Perry Morrison, *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*, second edition, MIT Press, 1994, p. 4.

51 Peter G. Neumann, "Inside Risks: Risks on the Rails," *Communications of the ACM*, July 1993, 36:7, p. 130, and *Computer-Related Risks*, p. 71. Although I take issue with some particulars, Neumann's Risks Forum, articles, and book are invaluable sources of information and analysis about risks in computer systems.

52 Amanda Bennett, "Strange 'Science': Predicting Health-Care Costs," *Wall Street Journal*, Feb. 7, 1994, p. B1.

53 Cynthia Crossen, "How 'Tactical Research' Muddied Diaper Debate," *Wall Street Journal*, May 17, 1994, pp. B1, B9.

54 Richard P. Turco, Owen Toon, Thomas Ackerman, James Pollack, and Carl Sagan, "Nuclear Winter: Global Consequences of Multiple Nuclear Explosions," *Science*, Dec. 23, 1984, p. 1284. Russell Seitz, "In From the Cold: 'Nuclear Winter' Melts Down," *The National Interest*, Fall 1986, pp. 3–17. Howard Maccabee, "Nuclear Winter: How Much Do We Really Know?" *Reason*, May 1985, pp. 26ff.

55 *Against the Gods: The Remarkable Story of Risk*, John Wiley & Sons, 1996, p. 16.

56 The main sources for this section include J. O. Hallquist and D. J. Benson, "DYNA3D–An Explicit Finite Element Program for Impact Calculations," in *Crashworthiness and Occupant Protection in Transportation Systems*, T. B. Khalil and A. I. King, eds., American Society of Mechanical Engineers, v. 106, p. 1. William H. Allen, "How To Build a Better Beer Can," pp. 32–36, and "DYNA Gets to the Heart of the Matter," p. 36, both in *Supercomputing Review*, March 1991. Steve Wampler, "DYNA3D: This Computer Code Seems to Offer Something for Everyone," *The Quarterly*, Lawrence Livermore National Laboratory, Sept. 1989, 20:2, pp. 7–11. "Motorists, Pedestrians May Find LLNL Computer Code a Life-Saver" and "LLNL Computer Code Makes the Jump from Modeling Machines to Man," news releases from Lawrence Livermore National Laboratories, March 7, 1991 (NR-91-03-01 and NR-91-03-02).

57 Thomas Frank And Karl Gruber, "Numerical Simulation of Frontal Impact and Frontal Offset Collisions," *Cray Channels*, Winter 1992.

58 J. T. Houghton *et al.*, eds., *Climate Change 2001: The Scientific Basis*, 2001; J. T. Houghton *et al.*, eds., *Climate Change 1995: The Science of Climate Change*, 1996; J. T. Houghton, B. A. Callander, and S. K. Varney, eds., *Climate Change 1992: The Supplementary Report to the IPCC Scientific Assessment*, 1992; J. T. Houghton, G. J. Jenkins, and J. J. Ephraums, eds., *Climate Change: The IPCC Scientific Assessment*, 1990; all published by Cambridge University Press. I also used a large variety of other books and articles for background. A book by climatologists critical of the models is included in the references at the end of the chapter.

59 D. L. Albritton and L. G. Meira Filho *et al.*, "Technical Summary," in J. T. Houghton *et al.*, eds., *Climate Change 2001*, pp. 21–83; see p. 37.

60 Albritton and Meira Filho *et al.*, "Technical Summary," p. 49.

61 Houghton *et al.*, *Climate Change 1992*, pp. 17, 139. Patrick J. Michaels, *Sound and Fury: The Science and Politics of Global Warming*, Cato Institute, 1992, pp. 114–118. "Technical Summary," *Climate Change 1995*, p. 27.

62 B. J. McAvaney *et al.*, "Model Evaluation," in J. T. Houghton *et al.*, eds., *Climate Change 2001*, pp. 471–523; see p. 473.

63 Stephen Schneider, quoted in Jonathan Schell, "Our Fragile Earth," *Discover*, Oct. 1989, pp. 44–50.

64 Forester and Morrison, *Computer Ethics*, pp. 4–5.

65 Bruce Stutz, "The Landscape of Hunger," *Audubon*, March/April 1993, pp. 54–63; see p. 62.

BOOKS AND ARTICLES

- W. Robert Collins, Keith W. Miller, Bethany J. Spielman, and Phillip Wherry, "How Good Is Good Enough?" *Communications of the ACM*, Jan. 1994, 37:1, pp. 81–91. A discussion of ethical issues about quality for software developers.

- Richard Epstein, *The Case of the Killer Robot*, John Wiley and Sons, 1996.
- Richard P. Feynman, *What Do You Care What Other People Think?*, W. W. Norton & Co., 1988. Includes Feynman's report on the investigation of the explosion of the Challenger space shuttle, with many insights about how to, and how not to, investigate a system failure.
- Jonathan Jacky, "Safety-Critical Computing: Hazards, Practices, Standards, and Regulation," in Charles Dunlop and Rob Kling, eds., *Computerization and Controversy*, Academic Press, 1991.
- Thomas K. Landauer, *The Trouble With Computers: Usefulness, Usability, and Productivity*, MIT Press, 1995.
- Nancy G. Leveson, *Safeware: System Safety and the Computer Age*, Addison Wesley, 1995.
- Nancy G. Leveson and Clark S. Turner, "An Investigation of the Therac-25 Accidents," *IEEE Computer*, July 1993, 26:7, pp. 18–41.
- Patrick J. Michaels and Robert C. Balling Jr., *The Satanic Gases: Clearing the Air about Global Warming*, Cato Institute, 2000. Michaels and Balling are climatologists critical of the climate models.
- Peter G. Neumann, *Computer-Related Risks*, Addison–Wesley, 1995.
- Peter G. Neumann *et al.*, "Inside Risks," *Communications of the ACM*, regular column, on the last page of each issue.
- Jakob Nielsen, *Designing Web Usability: The Practice of Simplicity*, New Riders Publishing, 2000.
- Donald Norman, *The Invisible Computer: Why Good Products Can Fail, the Personal Computer Is So Complex, and Information Appliances Are the Solution*, MIT Press, 1998.
- Donald Norman, *The Psychology of Everyday Things*, Basic Books, 1988. A study of good and bad user interfaces on many everyday devices and appliances.
- Effy Oz, "When Professional Standards Are Lax: The CONFIRM Failure and its Lessons," *Communications of the ACM*, Oct. 1994, 37:10, pp. 29–36. A study of a $125 million project that was canceled.
- David Parnas, "SDI: Violation of Professional Responsibility," *Abacus*, Winter 1987, pp. 46–52.
- Ivars Peterson, *Fatal Defect: Chasing Killer Computer Bugs*, Times Books (Random House), 1995.
- Henry Petroski, *To Engineer Is Human: The Role of Failure in Successful Design*, St. Martin's Press, 1985.
- Shari L. Pfleeger, *Software Engineering: Theory and Practice*, second edition, Prentice Hall, 2001.
- Jeffrey Rothfeder, *Privacy for Sale*, Simon & Schuster, 1992. Although the main focus of this book is privacy, it contains many examples of problems that resulted from errors in databases.
- Ben Shneiderman, *Designing the User Interface: Strategies for Effective Human–Computer Interaction*, third edition, Addison Wesley Longman, 1998.
- Edward Tufte, *Envisioning Information*, Graphics Press, 1990.
- Edward Tufte, *Visual Explanations*, Graphics Press, 1997.
- Aaron Wildavsky, *Searching for Safety*, Transaction Books, 1988. On the role of risk in making us safer.

ORGANIZATIONS AND WEBSITES

- Peter G. Neumann, moderator, *The Risks Digest: Forum on Risks to the Public In Computers and Related Systems*, archived at catless.ncl.ac.uk/Risks; current issue at www.csl.sri.com/~risko/risks.txt