Whatever Happened To Y2K? Using A Premier Crisis Management Prototype To Study Post 9/11 Preparedness

Elia Chepaitis
Information Systems and Operations Management
Fairfield University
Fairfield, CT 06430, USA

Abstract

Few topics interest students as much as emergency prevention and preparedness, particularly since the release of the 9/11 Commission's recommendations in the summer of 2004. This paper describes how the Millennium Crisis can be used to add models, linearity, context, research directions, and depth in this area. The author examines the pedagogical relevance of the features, impacts, contextual analysis, research opportunities, and lessons of the Y2K experience in emergency management discussions.

The Year 2000 crisis was a unique maintenance problem, not only of lasting importance for the information systems profession, but also for economic, socio-cultural, and political impacts. Invaluable lessons can be gleaned from this ubiquitous, temporal, costly, and successful campaign. The $600 billion debugging regime was a milestone achievement in information systems, and also provides a contemporary opportunity for critical analysis in fecund research areas: the economic impacts of massive information and communication technology investments, the acceleration of trends in systems analysis and design such as enterprise resource planning, and, most of all, for the implosion or dismantling of preparedness programs and the implications for post- 9/11 crisis response and management.

Numerous features of the Y2K campaign can be re-examined by students, academics, and practitioners, and perhaps resurrected--particularly collaboration across organizations to prevent or manage systems failures. Yet, Y2K has hardly been examined by scholars, policy makers, or disaster preparedness think tanks since the Millennium. This paper surveys first, the importance of Y2K for crisis management studies, and second, the significance of the popular perception that the Y2K crisis was exaggerated. The author briefly describes the available literature, the utility of Y2K as a stimulating addendum for EM classes in view of 9/11, and suggests areas for further investigations into emergency management models and opportunities.

Keywords: Y2K, crisis prevention, collaboration, prototype, emergency management (EM)

1. INTRODUCTION

Numerous aspects of the Y2K crisis add depth and linearity to emergency management (EM) education. Although Y2K was regarded in 2000 as a unique, "stand-alone" event, the Millennium Projects are valuable as a prototype, an example of the importance of context, and an occasion to trace both continuity and also discontinuity in systems development. The socio-cultural and political context of Y2K is dramatic and arresting, and generates rewarding classroom discussion and research projects.

To most laymen, the year 2000 crisis is remembered as a comic non-event, a patch job, characterized by confusion, mismanagement, hyperbole, and over-investment. Yet Y2K did matter since insights into crisis response and management theory and practice evolved and spread. Best practices were enhanced through inter-organizational brainstorming, in five distinct stages: anticipating

failure points and preventing crisis; planning for the response to a crisis situation; training for a crisis, including organizing and rehearsing crisis exercises; and, finally, evaluating the performance during and after the crisis.

Y2K positioned information systems within a wider, novel context and the broader view of systems and subsystems produced industry-wide reviews of information environments and of the repercussions of system failures. Government leaders, bureaucrats, managers, and professionals at every level gathered, often in public televised forums, to discuss testing, readiness, and remediation. Information systems responsibilities spread across a broad range of players, from Chief Information Officers (CIOs) to congressional committees to the Securities and Exchange Commission.

Although Y2K was, to some extent, an exercise in media hype and professional showboating, the Millennium projects represented a leap forward in multi-party risk analysis, data quality control, and contingency planning. Y2K prevention required coordinated efforts, resource allocation, and commitment that were truly global. The reach of the Y2K crisis was universal: from government to transportation to communication, banking, military, healthcare, educational, and utilities, and through local restaurants, dentist's offices, retailers, and libraries. Prevention and preparedness programs improved crisis management primarily and permanently within organizations, but not necessarily across super systems.

The response to the crisis was, of necessity, huge: "the largest coordinated worldwide activity to address a shared technology problem », according to IS guru Keith Jones (McDermott, 42). Olympic preparations, hyperinflation, the conversion to the Euro, and other landmark challenges could not compare to Y2K.

FEMA (the Federal Emergency Management Agency), the Securities and Exchange Commission, government at all levels, banking regulators, transportation authorities, and local militia and health organizations not only joined in the cooperative effort, but were themselves forced to demonstrate Y2K readiness. Although special teams and committees were disbanded after the event, the Millennium Crisis left some legacies. Y2K projects illustrated that in future crises, information and communication systems (ICTs) stability required the commitment, participation, education, intelligence, and resource management of multiple classes of stakeholders.

2. THE RELEVANCE OF Y2K'S SHORT-TERM IMPACT FOR EM EDUCATION

Both investments in emergency preparedness, and also cross-systems approaches to disaster and contingency planning produced multiple impacts (Table 1). The aggregate effects of coordinated attention to legacy systems in areas such as utilities, transportation, banking and finance, healthcare, and government were monumental. IT acceleration and coordination due to Y2K produced multiple impacts: $600 billion, (a figure widely quoted, by the Gartner Group) spent on testing; a plethora of outsourcing partnerships; investment in debugging and upgrading; and productivity increases in the short and in the long term. The IT-driven productivity surge of the late 1990s drove the U.S. stock market to unprecedented heights, although over investment in IT produced a novel but dangerous business cycle. Economically, Y2K readiness could not be assured through domestic efforts alone. Outsourcing gathered steam--from SAP in Germany to shops throughout Bangalore, India.

Technologically, the major impacts of the Year 2000 crisis linked seven areas: systems analysis and design, accelerated systems upgrading and platform choices, upgraded 1997-2000 IT budgets, changes in authority for control and maintenance, the emergence of major global software players and partnerships, and an enhanced public understanding of ICTs as systems.

Y2K accelerated the development of Application Service Providers and Enterprise Resource Planning, and paved the way for the emergence of Chief Security Officers (CSOs) to manage disaster preparedness for business enterprises. Ironically, although ICTs were the problem, they also emerged as the solution. Unprecedented cross-disciplinary teamwork, oversight, development and systems-wide assessment prevented significant system failures on time, although often vastly over budget.

Professional
an enforced deadline
surge in outsourcing
replacement of legacy systems
teamwork and accountability
humility
Economic
$600 billion invested [Gartner Group]
surge in upgrade funds tech stock market bubble
competitive advantage
Sociocultural
consistent, dramatic newsworthiness
ongoing debate about risks
popular stake in preparedness
subject for humor, hype, and skepticism
a global event
Political
oversight and responsibility
executive, SEC, legislative
hearings, judiciary
both non-profit and commercial command & control regimes
Intellectual
unprecedented attention to ICTs
acknowledged dependence on overlapping systems
debate on the general good and IT
Multiple Impacts of the Y2K Crisis
Table 1

Economically and financially, trends in IT investment from 1995 to 2000 seem to show that over investment in Y2K contributed to the bubble in the stock market and post-2000 the recession. Coincidentally, a letter in *Business Week* (March 15, 2004) by John Hoagland of Michigan State supports this hypothesis. Two other factors probably reduced employment, from manufacturing to services: increases in productivity because of IT installed during the Y2K crisis, as well as expanded outsourcing that originated with Y2K projects.

Students are invited to rank and discuss the most important effects of Y2K: intellectual, financial, technological, economic, and sociocultural. Many find that Y2K was, above all, educative. The event enlarged the criteria for sound information systems practice, and extended the arena of responsibility, accountability, and liability away from small circles of systems professionals: to manufacturers, chip designers, industry analysts, management at every level, users, sociocultural gurus, economic analysts, and political leaders.

In the U.S., government required corporations to certify their compliance Y2K readiness standards through the Securities and Exchange Commission.

Intellectually, Y2K educated policy makers, the public at large, and business leaders about risk as no other event before or since. Scenarios were investigated and replayed across the world: the impacts of systems failure were quantified and the ripple effects fully described—sometimes to excess, with socio-cultural as well as technological impacts. The number of stakeholders in information systems reliability was, for the first time, perceived to be nearly universal in advanced economies. Financially, outlays for systems upgrades and replacement totaled over $20 billion, and promoted a willingness to fund permanently financial commitments for maintenance and continuation in cases of unanticipated disasters.

From systems forensics to desktop information responsibility, the debate promoted widespread understanding and agreement: of dependence on information systems, of vulnerability to attack or sabotage, of the costs of downtime and disruption—ranging from spoiled food to the health implications of disabled transportation and delivery systems.

Particularly in view of the 9/11 Commissions recommendations, students are often struck by Y2K's contribution to collaborative enterprise development in the private sector, in contrast with the lack of integration and extension across government agencies.

3. LITERATURE REVIEW

From 1995 up to 2000, paralleling and fueling the interest in Y2K in the media, a significant body of literature emerged: monographs, articles, Senate hearings, the Securities and Exchange Commission's compliance documents, and trade publications. Three monographs were prominent in the late 1990s: Hyatt's *The Millennium Bug: Survive the Coming Chaos* (1998)*, Yourdon's*

and Yourdon's Time *Bomb 2000* (1998), and McDermott's *Solving the Year 2000 Crisis* (1998). Yourdon and Yourdon stated that their's was not a book for professionals, and focused on coping with potential Y2K breakdowns : billing, shortages, disruption and destruction of pieces of the infrastructure. Their dire scenarios are summarized and graphically presented for EM discussions in 2004-5 courses. Students can grasp the interdependence of systems and a viable infrastructures through these doomsday scenarios.

The Yourdons investigated the potential impact on various industries, and Hyatt's book was not only a survival guide, but also contained estimates of the costs of software fixes and the potential costs of institutional breakdowns if there were still software glitches because of Y2K.

Two videos of a conference on the Year 2000 Problem, hosted by the Center for Stategic and International Studies, and broadcast over C-Span, are archived at Purdue University's Public Affairs Video Archives.

McDermott's monograph offered a superb overview of software and hardware options and costs. The choices that students weighed were: replace, expand, window, compress, work around, encapsulate, and abandon. The classes benefited immensely from all the rich and current material, including humor and satire, that was available. They researched and presented excellent projects on transportation systems, government readiness, banking and finance, communications, and health care risks. We used McDermott for a textbook, since his emphasis was on computer engineering and excellent for systems analysis and design, but both Hyatt's and the Yourdons' more sensational materials provided provocative supplementary materials.

Unfortunately, these books are dated, and of limited value for an assessment of the significance of Y2K beyond the Millennium. After the Millennium, almost nothing of substance was published on Y2K. Since 2000, no monographs and few scholarly articles on Y2K itself were published. It was as though the Y2K crisis was an embarrassment, a distraction for the public that is best forgotten. The few Y2K failures did not have disastrous consequences, were speedily repaired, and were not reported at length.

The long-term effects of Y2K on emergency response, back-up systems, auditing and oversight are discussed cursorily in engineering, retailing, healthcare, and information systems periodicals, but not in refereed articles. The bibliography lists some recent trade literature. Significant material can be gathered for this research from a variety of non-academic sources, such as the Department of Commerce's data on aggregate IT investment from 1995 to 2000, and readily available GDP data. Finally, isolated comments and case studies, such as *Nestle Struggles with Enterprise Systems* (Laudon and Laudon, 2004) mention the deleterious impact of diverting funds from ERP (enterprise resource planning) to the Y2K crisis. These and other small accounts in the aggregate offer important clues to the opportunity costs of Y2K funding.

The absence of research after 2000, the disbanding of special commissions, and the end to the Security and Exchange Commission's oversight suggest a lack of long-term focus and creativity, and interests classes, especially in light of the *9/11 Commission Report (2004*).

4. Y2K AS A VIABLE CONTEMPORARY MODEL

Whether, for example, Y2K illustrates that we create systems that we don't understand, or as an example of unprecedented but short-term collaboration, Y2K is an interesting prototype and model for EM. The unique attention devoted to multiple failures and ripple effects is the only "walk-through" scenario to date that has come close to mimicking the devastation that could be caused by cyberterrorism, for example.

Moreover, as Table 2 illustrates, crisis prevention, response, and emergency management across multiple organizations were effectively and cogently linked as never before. Not only command and control regimes, but also lateral contingency plans were constructed. From the Securities and Exchange Commission to customers, organizations were pressured to achieve and document their readiness and compliance with government guidelines. Some used this readiness for competitive advantage, to reassure customers that Y2K would not threaten their savings, destroy their creditworthiness, erase their patient records, or

cause elevators and security systems to trap them in dark and airless places.

Unlike previous and future crises, the problem was anticipated and an enforced deadline was observed, although no one knew just how many systems and embedded chips were vulnerable. This ubiquitous Y2K effort forced organizations and individuals to garner resources, to perform system-wide analyses, and to replace unreliable legacy systems in a timely manner over a multi-year time frame, and to confess, before the congressional Y2K commission, "We have created systems we don't understand (Hyatt, 108)." Although Y2K was not a security problem *per se*, but a maintenance issue, the effects on security investment and planning were deep and far-reaching. Not only information systems professionals, but also leaders and professionals in every application area saw computer systems as subsystems of their areas of responsibility and accountability. The acknowledged dependence of government, services, healthcare, utilities, transportation, and communications on reliable information systems widened the circle of stakeholders for crisis prevention, response, and management.

Salient and cogent questions surface in multiple disciplines. Strategically, how can Y2K regimes be tailored to tackle the security and performance problems of the 21st century? Tactically, how can inter-organizational collaboration and oversight be restored for disaster preparedness? Other questions are: would outsourcing, the movements toward enterprise resource management and application service providers, and the replacement of legacy systems have been unlikely or merely delayed in the absence of Y2K investments, contingency plans, and ITC staff empowerment? In which industries or institutions was compliance, resistance, or upgrading most typical, and why? What was the precise impact of the billions of dollars spent on testing, debugging, and upgrading: on productivity and on the business cycle--in the short and in the long term? How much did the IT-driven productivity surge propel the U.S. into global economic leadership, followed by a subsequent "bubble" and relative decline? Most of all, who in EM, beyond the organization, is responsible and accountable for the general good?

Prevention:
- preparedness and oversight:
  - command & control regimes
  - documented Y2K readiness, certification, compliance
  - a deadline: ease of definition

Communication:
- multidirectional, dramatic, dynamic
- inter-organizational cooperation & collaboration
- accountability, responsibility , & liability established

Response:
- risk analysis
  - multilevel ripple effects
  - contingency planning
  - flexibility
  - informed oversight
  - massive IT investments
- Emergency Management
  - multi-level political & commercial leadership

Millennium Projects: Critical Linkages, from Prevention through Emergency Management

Table 2

5. SOCIOCULTURAL FACTORS AND LOST OPPORTUNITIES

A linear view of Y2K regimens before and after the Millennium provides an instructive and cautionary snapshot of the importance of leadership, communication, and public attitudes toward EM. Ironically, although numerous upgrades and contingency plans were completed, especially in the private sector, many valuable features and insights were abandoned swiftly after the Millennium. Why, on the whole, were emergency preparedness and inter-organizational approaches to disaster and contingency planning enhanced only temporarily by the ubiquitous multi-year Y2K effort?

ICT investment, learning, leadership, and commitment in information systems control occurred as a result of Y2K, yet the event then and now is often popularly recalled as an embarrassment and a hyped media event. This impression is significant.

The dominant Y2K question on January 1, 2000 was, "Why was the crisis exagger-

ated?" The author believes that this was the wrong question, but a profoundly important question. [A more constructive question would have been: "Why did Y2K succeed, and what can we borrow from those crisis management regimes?"] The perception, one that may be correct, that the Y2K threat was exaggerated had significant consequences, notably in disaster preparedness. Disaster preparedness gurus fed this impression.

What to Do

1. Secure copies of important documents
2. Build an emergency preparedness library
3. Distinguish edible plants from those that are deadly
4. Evaluate your current location
5. Determine your self-defence philosophy. If you are going to purchase agun, make sure it is appropriate for your size and goals
6. Find an alternate source of water
7. Stockpile food and common household goods
8. Purchase adequate clothing (because the Y2K crisis will start in the middle of winter)
9. Develop an alternate source of heat and energy. If you don't have a fireplace, you might consider putting in a woodburning stove
10. Prepare an emergency medical kit
11. Determine how you will dispose of waste
12. Secure an alternate form of currency
13. Aquire a basic selection of hand tools

---

from *The Millennium Bug: How to Survive the Coming Chaos* (Hyatt, 210).

Chart 1

Chart 1, "What to Do" from Hyatt's *The Millennium Bug: How to Survive the Coming Chaos* presents typical, fearful scenarios to the public. These doomsday warnings may have distracted the population from more constructive and long-term advice: a lesson for future EM programs.

Hyatt added, " I would suggest stockpiling: ammunition (especially 22 caliber), toilet paper, Bic lighters, coffee and tea, sugar" (Hyatt, 210). Table 3 lists chapter topics in *Time Bomb 2000*; each chapter included contingency plans, or fall back advice for two days, one week, a month, a year, or ten-year failures.

Since Y2K had the potential for grave damage to vast super systems, to elevators, to air traffic control, to public utilities, to security systems themselves, the public's attention seldom wavered. Unfortunately, popular interest in systems and risk containment was shallow and transient—possibly because of sensationalism. Before and after the crisis, not only the event, but also the publicity surrounding the event, transformed disaster preparedness and the public awareness of crisis management. Some benefits did survive, such as cross system contingency planning (Table 3). Also the viability of the ICT infrastructure emerged as an area of policy and concern not only for individual organizations but also for the general good.

banking/finance
communications
education
embedded systems
food
government
jobs
news/information
health services
retailers
transportation
telephone and mail systems
utilities

Critical and Overlapping Systems Examined, with Fall Back Positions (*Time Bomb 2000* , Yourdon and Yourdon)

Table 3

In addition to waning popular support, why else did Y2K regimes implode to such a great extent after January 1, 2000? The crisis was well defined, with an immutable deadline, and the problem was perceived more as a singular maintenance event than part of an ongoing security regimen. As Table 4 illustrates, numerous professional, economic, socio-cultural, and political factors contributed to the implosion of Y2K projects after

January 1, 2000. Budgets were exhausted, IS gurus and pundits were ridiculed, little political capital or leadership could be generated to continue nation-wide disaster preparedness.

Professional
success but embarrassment
collaboration and cooperation ends
new IT foci: ASPs, ERP
Economic
budgets exhausted
IT bubble
competitive advantage elsewhere
Sociocultural
ridicule
fickle audience
sharp decline in newsworthiness
credibility issue
Political
lack of political will, expertise & imagination
divorce of Y2K from issues, especially in regard to cyberterrorism
regimes dismantled: difficult communication
poor definition & oversight
separation of public & commercial issues
atrophy of cooperation
dismantling of command & control regimes
Intellectual
splintered & competing views of the general good

Why Y2K Readiness Imploded

Table 4

Yet critical collaboration generated during the Y2K crisis between both non-profit and commercial organizations dissipated. (See Table 4). Even the terrorist attacks of 9-11 did not stimulate interest in Y2K methods and models. Much commonality of interest between government and business in EM evaporated further after the passage of the Patriot Act (Houle *et al,* 2004).

In sum, did media hype and "popular wisdom" obscure numerous collateral benefits of the Y2K crisis that deserve attention--such as system-wide understanding of IT possibilities and relationships that emerged or were at least accelerated by Y2K investments and contingency plans? Although damage from the Millennium Bug was undoubtedly overestimated, the shibboleth of Y2K as a non-event and a temporary diversion deserves to be challenged.

6. CONCLUSION

From hactivists (Childress, 2004) to cyberterrorists, students are bombarded continuously with problems of control. In the MIS syllabus for the fall of 2004, the author refers to security as "the 800 Pound Gorilla."

Unlike most crises, Y2K was not an accident or an unanticipated event, and the problem and its solution were well publicized and documented before the event. Yet the Millennium bug remains dramatic and relevant not only for crisis response and management, but also for crisis prevention in 2004. Students are impressed that the multi-year response to Y2K was well orchestrated and productive. The simultaneity, high stakes, and ubiquity of the Millennium crisis permanently expanded the circle of players with vested interests in and responsibility for systems failures.

From government agencies to households, users realized that responsibility for information systems design and control must extend beyond computer engineers and information systems professionals, to ensure the general good. Therefore, a review of Y2K provides a superb opportunity for critical thinking. The problem generated well-deserved humility within the profession--because IT professionals did cause the problem, and could definitively say how many systems were affected. The significance of the cross-disciplinary context cannot be overstated. In this case, the most impressive impact on students is the critical socio-cultural factor--the damaging impact of short-term perceptions that probably diluted the intelligence and will to invest in more variable, long-term readiness.

In hindsight, Y2K probably proved that in future crises, such as a cyberterrorist attack, successful preparedness requires leadership, popular communication, widespread and measurable commitments, participation,

education, intelligence, and resource management by multiple classes of stakeholders. Experts can acknowledge that the gravity and scope of threats are uncertain, but attempts at definition and walk-throughs are vital. Like Y2K, the responders to crises must be broad based , well funded, and knowledgeable. FEMA (the Federal Emergency Management Agency), the Securities and Exchange Commission, government at all levels, banking regulators, transportation authorities, and local militia and health organizations not only joined in the cooperative effort, but were themselves forced to demonstrate Y2K readiness.

Although special teams and committees were disbanded after the event, Y2K as a prototype left interesting if disparate legacies for disaster preparedness and crisis management. In addition, the impact of the general consensus after Y2K, that the Year 2000 crisis was overstated, also informs students. Leadership, investment, and collaboration regimes evaporated, although theses might have been adapted to meet subsequent challenges, such as cyberterorism or the failure of the electrical grid in the eastern half of the United States in August 2003.

For teaching and research, Y2K raises important questions in at least three other areas:

1. Systems analysis and design:

   a. Did Y2K accelerate the replacement of legacy systems, often in favor of new IT platforms?

   b. Did the projects change the control and maintenance function within enterprises and nonprofits?

2. The economy

   a. What was the impact of ramped up 1997-2000 IT budgets and Y2K priorities on the business cycle 2000-2003?

   b. How did Y2K promote the emergence of major global software players and partnerships, particularly in outsourcing for application service providers, and enterprise resource planning?

3. The impact on organizations and society beyond IT professionals.

   a. Did the wide circle of stakeholders caught up in the Y2K crisis lead to more shared responsibility, accountability, and liability for systems control and security?

   b. What was range of the popular responses to the Y2K non-crisis, and are these significant?

4. What lessons does the Y2K experience offer for disaster preparedness, especially against cyberterrorism? A list presentation of unexplored research topics empowers students. Also, what we know and what we don't know are of equal importance in the field—especially as we move closer and closer to issues that affect the general good.

A number of additional research paths are open and non-trivial. What were the multidisciplinary consequences when organizations and users took ownership of information systems after professionals confessed that, as a whole, they had erred? What did we learn and what did we not learn? Who learned, and who is still building on the Y2K prototype? What concrete changes and contributions can be attributed to Y2K, however inadvertently, and which opportunities may have been missed? For whom? How can the problem of the Millennium be compared and contrasted with contemporary threats?

The author wishes to thank Fairfield University's Research Committee for their generous support for this project.

7. REFERENCES

Chepaitis, E. (2004) "The Impact of Y2K on Crisis Management: Widening the Stakeholder Circle for Crisis Prevention and Response." Proceedings: Information Systems Response and Management (ISCRAM) Conference. Brussels, 2004.

Childress, S. (2004). *"Hactivists Log On: Police Are On Guard against Threats of Electronic Chaos".* Newsweek . (August 30), 43.

Elliott, H., "No Bugs; Now What*?* "(2000). Electronic News.1/10/00 v. 46(2), pp.32-35.

Harrington, R. ((2000). "Lessons Learned from Y2K*"*. Credit Union Executive Journal. 40(1), 6-10.

Henderson. T. (2000) "Retailers to Press On with Projects Deferred by Y2K*"*. Stores Magazine. 82(1), pp.138-140.

Hulme, G. V., Garvey, M.J., and Rendelman, V. (2002). *The Right Balance: National Cybersecurity Plan Takes Shape but Raises Questions about Expectations*. Information Week. (September 16), pp.22-23.

Hyatt, M. (1998). The Millennium Bug: Survive the Coming Chaos. Washington, DC: Regnery.

McDermott, P. (1998). Solving the Year 2000 Crisis. London: Artech House.

Moran, J. M. (2004). *Crisis Preparations Lack 9/11 Urgency.* Hartford Courant. (September 11), pp. A1, A9.

National Commission on Terrorist Attacks upon the United States *. The 9/11 Commission Report*: *Final Report of the National Commission on Terrorist Attacks upon the United States.* (2004) N.Y.: W. W. Norton & Co.

"No News Is Good News" (2000). Engineering News-Record. 244(2), pp. 60-62.

"Now That It's Over, Was the Y2K Effort Worth It?" (2000). Editorial. National Underwriter/Life and Health Financial Services. 104(9). 2/28. p. 18-21.

Purnelle, A. , " A Now-Unemployed Y2K Warrior Reflects" (2000). Byte.com. 1/10/2000.

Vandersluis, C. (2000) "Time to Give Secondary Systems Y2K Makeover". Computing Canada. 26(2), pp. 22-24.

"Year 2000 Market Opinion". (2000) Pure Fundamentals 9(1), pp.1-2.

Yourdon,E. and Yourdon, J. (1998) Time Bomb 2002. NY: Prentice Hall.