THE IMPACT OF Y2K ON CRISIS MANAGEMENT
Widening the Stakeholder Circle for Crisis Prevention and Response

Elia Chepaitis
Information Systems and Operations Management, Fairfield University, Fairfield, CT 06430
E-mail: echepaitis@mail.fairfield.edu

Keywords: Y2K, stakeholders, crisis prevention

Abstract: Although Y2K was neither an accident nor an unanticipated challenge, the millennium debugging represented a watershed event for crisis response and management, and the range of effects remains relevant in 2004. 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, healthcare, utilities, transportation, services, and communications on reliable information systems widened the circle of stakeholders for crisis prevention, response, and management. Emergency preparedness and broad systems approaches to disaster and contingency planning were enhanced by the ubiquitous multi-year Y2K effort. The author emphasizes the investments, learning, leadership, and commitment in information systems control that occurred as part of the prevention stage of crisis management as a result of Y2K. The simultaneity, high stakes, and ubiquity of the millennium crisis permanently altered the circle of players with vested interests in and responsibility for information systems control. From government agencies to households, users realized that the scope of information systems design and reliability must extend beyond computer engineers and information systems professionals to ensure the general good.

1 INTRODUCTION

Unlike most crises, the Y2K crisis was not an accident or an unanticipated event. Yet the millennium bug remains relevant not only for crisis response and management, but also to crisis prevention in 2004. 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. Both massive investments in emergency preparedness, and also multiple-systems approaches to disaster and contingency planning left invaluable significant legacies for crisis management. 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.

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 unprecedented system-wide analyses, and to replace unreliable legacy systems in a timely manner over a multi-year time frame. 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.

2 CRISIS PREVENTION

Insights into crisis response and management theory and practice evolved and spread, and best

practices were enhanced through inter-organizational brainstorming, for 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. This research emphasizes the first stage: anticipation and prevention, and the impact of these two activities on preparedness, procedures, and multiple levels of stakeholder responsibilities.

Y2K positioned information systems within a wider, novel context and this expanded view increased not only the stakes of failure but also the types of stakeholders dedicated to preventing failure. The broader view of systems and subsystems produced industry-wide reviews of information environments and of the repercussions of system failure.

3 THE STAKEHOLDERS

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.

The scope, depth, and ubiquity of the Y2K problem captured the public imagination and remains unprecedented. 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 and, inadvertently, the popular understanding of risk containment spread. Before and after the crisis, not only the event, but also the publicity surrounding the event, transformed disaster preparedness, and preventative measures improved crisis management permanently.

Although the Y2K crisis was, to some extent, an exercise in media hype and professional showboating, Y2K campaigns represented a huge leap forward in multi-party risk analysis, data quality control, and contingency planning. Moreover, 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.

Because the response to Y2K was unprecedented and a multi-year event, the effort was unique not only in scope and investment, but also in the number of stakeholders permanently involved in systems control. The response to the crisis is instructional: 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 left broad and lasting 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 and practitioners.

4 IMPACTS

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: billions of dollars spent on testing; a plethora of outsourcing partnerships; massive 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 overinvestment 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. In the U.S., corporations were compelled to certify their compliance with the Securities and Exchange Commission.

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.

Although Y2K failures were modest and below expectations, Y2K mattered. We are still assessing the multiple effects of Y2K: intellectual, financial,

technological, economic, and socio-cultural. 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, socio-cultural gurus, economic analysts, and political leaders. From systems forensics to desktop information responsibility, the hype promoted widespread understanding: 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.

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.

5 CONCLUSION

Ironically, although ICTs were the problem, they also emerged as the solution. Unprecedented cross-disciplinary teamwork, oversight, development and systems-wide assessment were required. This author will discuss not only the tools and resources mobilized for the design, development, and deployment of both Y2K ready systems, but also contingency and continuity programs, teams, and emergency resources. The important questions raised in this research are: What did we learn and what did we not learn from Y2K? Who learned? What concrete changes and contributions can be attributed to Y2K, however inadvertently, and which opportunities may have been missed? For whom? In the long term, media hype obscured numerous collateral benefits of the Y2K crisis--such as unprecedented system-wide understanding of IT possibilities and relationships that emerged or were at least accelerated by massive Y2K investments, contingency plans, and stakeholder empowerment.

REFERENCES

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.

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

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

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.