POLICY FORUM: TECHNOLOGY

The Y2K Problem

Robert F. Bennett

The Year 2000 (Y2K) technology problem is a crisis that threatens critical operations of the U.S. government, our economic strength, and vital connections with the global community. It is a collective crisis born from executive-level deferment and neglect, compounded by unwillingness to share information and an absence of verifiable assessments of technological preparedness. Exploited by fearmongers and profiteers, the problem has spawned a cottage industry preying on fears that "the end is nigh." Others claim it is a hoax by information technology designers.

The Y2K problem is real, caused by an outmoded, two-digit dating system in computer software and hardware that may knock vital systems offline on 1 January 2000. Although it is far from the end of the world, the interdependent nature of technology systems makes the severity of disruptions virtually impossible to predict.

In addition to the estimated $1.5 trillion global cost of dealing with Y2K (*1*), the ultimate consequences may play out for years in the forms of global recession and infrastructure collapse in developing nations. The problems arising from Y2K will not begin and end neatly on 1 January of the year 2000. According to L. Marcoccio of the Gartner Group, an international high-tech consulting firm, system failures due to Y2K have been occurring for some time (*2*). They will increase in 1999, reach their peak during 2000, and drop off in 2001. A few will continue past 2003.

> "Y2K provides an opportunity to understand the technological vulnerabilities that can arise from human shortsightedness."

There is a growing amount of information on the preparedness of some key industries and economic sectors. The electric utilities, for example, have cooperated in a Y2K readiness effort by the North American Electric Reliability Council (NERC) that released a comprehensive survey in January 1999 (*3*). However, many of the fundamental questions about risk and personal preparedness cannot be answered. Many organizations critical to Americans' safety and well-being are not fully engaged in finding a solution. According to the National Federation of Independent Business, a recent Gallup Organization survey revealed that more than 50% of small and medium-sized businesses that use computers or microchip-based devices have yet to address the problem (*4*). Nearly all affected industries and organizations started Y2K remediation too late. As a result, most organizations must exercise "triage"—focusing on what is critical to sustain the life of an enterprise as opposed to finding long-term solutions.

Lawmakers in the 106th Congress face numerous challenges as they consider approaches to limiting Y2K's economic impact, safeguarding vital government services, and ensuring public safety. Among the biggest hurdles is the problem that self-reporting has become the standard in both private industry and government. With few exceptions, disclosure of Y2K compliance is poor. To encourage information sharing, the Senate Special Committee on the Year 2000 Technology Problem (referred to here as the Senate Y2K Committee) (*5*) spearheaded a bipartisan effort that passed the Year 2000 Information Disclosure Act (S. 2392) and the CRASH legislation (S. 1518) that led to a requirement by the Securities and Exchange Commission for meaningful Y2K corporate disclosures to shareholders. Unfortunately, when self-reported facts have become subject to independent verification, the results have been mixed.

Another hurdle is that national emergency and security planning for Y2K-related systems failures is just beginning. There needs to be a national strategic plan to ensure the functioning of critical infrastructures and a contingency plan in the event of infrastructure collapse.

Furthermore, although the Office of Management and Budget has given federal agencies guidelines with which to determine what systems are mission-critical and how to report Y2K readiness levels, U.S. national efforts pale in comparison to those of Canada (*6*) and especially the United Kingdom, where the prime minister has taken a lead role in an enormous public information campaign (*7*).

Since its establishment in April 1998, the Senate Y2K Committee has held hearings and recently released a report (*5*). Although the situation is clearly changing rapidly, the following should be considered as preliminary assessments of eight vital economic sectors.

Utilities

The nation's electric power industry consists of 3200 independent utilities. Although most utilties have participated in a coordinated Y2K plan, overall remediation of the electric power industry is slow. The NERC has reported that as of the fourth quarter of 1998, only 44% of the industry's mission-critical equipment had even been tested (*3*). The committee has also been concerned that the approximately 1000 small rural electric utilities may not have sufficient resources to devote to Y2K compliance.

Compliance among oil and natural gas utilities is also progressing slowly. A survey by the committee (*5*), though limited in scope, indicates a lack of contingency planning, overly optimistic compliance assertions, and a lack of knowledge about suppliers' Y2K status. In a survey of 1000 oil and gas companies released on 18 February 1999, 86% reported that they were in the final stages of repair and testing. However, only about 50% of the retail gas stations report full compliance (*8*).

Although compliance efforts are behind, the utility industry as a whole is configured to handle interruptions, blackouts, and natural disasters. A prolonged nationwide blackout is not likely. Local and regional service outages, however, are distinct possibilities.

Health Care

The health care industry is one of the worst prepared for Y2K and carries the greatest potential for harm. Critical medical equipment (such as defibrillators or respirators), patient records, organizations providing medical supplies (such as of blood, drugs, linens, and bandages), and health care insurers are all in jeopardy. Because of limited resources and a lack of awareness, rural and inner-city hospitals are particularly at risk. According to a recent report by the American Hospital Association only 13% of the 583 hospitals surveyed are currently ready for the year 2000 (*9*).

The probability of malfunctions in medical devices is also cause for great concern. The Food and Drug Administration (FDA)

The author is a Republican senator from Utah and chairman of the U.S. Senate Special Committee on the Year 2000 Technology Problem. E-mail: year2000@y2k.senate.gov

has set up a Biomedical Equipment Clearinghouse Database so that manufacturers can provide information about Y2K effects on medical devices or laboratory equipment (*10*). However, the FDA is not making independent assessments, and there is no guarantee that a product is compliant if the manufacturer has not sent information.

Telecommunications

The United States has never experienced a widespread telecommunications outage, yet the telecom network is one of the most Y2K-vulnerable systems. For example, as reported to the president's National Security Telecommunications Advisory Committee, in a telecommunications company "there may be 400 to 1600 switches, 30 to 50 signal transfer points, 5 to 60 service control points, thousands of transport component systems, and many element management systems and operations systems, any one of which could have multiple date-sensitive functions" (*11*). Although 95% of telephone systems are expected to be compliant in time, there is no industrywide effort to test data networks, cellular and satellite communications systems, or the nation's 1400 regional telecom carriers. Despite telecom infrastructure readiness, customer equipment and company switchboards may experience problems, leaving no guarantee (for some) of getting a dial tone on 1 January.

Transportation

Although there is no reason to anticipate plane crashes, flight rationing to some areas and countries is possible. The Federal Aviation Administration (FAA) got a late start but has renovated the host microcode system that tracks domestic flights from the FAA's en-route carriers (*12*). The planes themselves are in good shape for Y2K. On average, however, the 670 domestic airports started Y2K compliance too late for on-the-ground systems such as baggage handling and security. The situation with international air traffic control and airports is much worse, and the maritime industry has not moved aggressively toward compliance for ships and ports. Some disruption of global trade is likely.

Finance

The financial services sector ranks ahead of nearly all other industries in remediation and testing. There are now legal requirements that dealer-brokers and publicly traded companies disclose Y2K compliance information. The unprecedented threat of litigation, however, has discouraged disclosure. Although only rough estimates of Y2K-associated litigation can be made, several groups have calculated total Y2K liability costs in the United States at $1 trillion (*13*). Federal regulators have made considerable progress in tracking compliance among banks, thrifts, and credit unions, of which 95% have received satisfactory government ratings. Banks and ATMs are expected to be functioning and have enough cash, thanks to a $50 billion order of extra cash by the Federal Reserve.

Government

Federal government Y2K preparations vary substantially. The President's Council on Year 2000 Conversion is submitting quarterly reports (*14*). The Social Security Administration got an early start and is well prepared; other agencies such as the Department of Defense and Health Care Financing Administration are lagging behind. The federal government will spend in excess of $7.5 billion for Y2K remediation, but the Senate Y2K Committee believes that it will not be able to renovate, test, and implement all of its mission-critical systems in time. After a late start, the Federal Emergency Management Agency is now engaged in national emergency planning in the event of Y2K disruptions (*15*), but many state and local governments are not prepared to deliver critical services such as benefit payments, responses to 911 calls, and emergency services.

General Business

Although the heavily regulated insurance, investment, and banking industries are farthest ahead in Y2K compliance efforts, health care, oil, education, agriculture, farming, food processing, and the construction industries are lagging behind. It is projected that the costs of regaining lost operational capability after mission-critical failures will range from $20,000 to $3.5 million (depending on the size of the company) and that the loss of capabilities will last at least 3 days (*2*). Large companies with greater resources are better able to deal with the Y2K problem. Small and medium-sized businesses, however, are the most vulnerable to Y2K disruptions.

International

Although several international organizations are involved in increasing awareness about the problem, including the United Nations, the World Bank, and the European Commission (*16*), some of America's major trading partners have not been taking the situation seriously and are not going to be ready for Y2K. Dire effects are predicted in developing countries, which may simply fall off the technological map. The fears of stockpilers and survivalists in some countries are not totally unfounded: There exists the likelihood of regional economic and civil unrest in regions already experiencing political instability, runaway inflation, and food and supply shortages. Those who suggest that it will be nothing more than a "bump in the road" are misinformed.

Conclusions

There are reasonable steps individuals can take to prepare for Y2K. Consumers should keep copies of financial statements and ask local banks what efforts are being made toward Y2K compliance. Employers, local elected officials, and utility providers should be contacted. Investors should obtain compliance information before making investment decisions, and those with pension funds should contact fund managers about Y2K vulnerabilities. Above all, we should prepare for Y2K on the basis of facts and reasonable predictions about the problem's effects on vital services.

As we count down the final months, it is unfortunate how little information is available. More independent verification of information on industry and government Y2K readiness is necessary to ensure public trust as we approach the new millennium, and therein lies the opportunity for assistance from the efforts of America's research and high-tech communities.

Globally, leaders of corporations and countries are struggling to understand the Y2K problem. In the process, they are receiving a crash course in the fragile mechanics of information technology. Y2K provides an opportunity to understand the technological vulnerabilities that can arise from human shortsightedness.

References and Notes

1. E. Luening, "Who will pay the bill," CNET NEWS.COM, 20 January 1999 (http://www.news.com).
2. L. Marcoccio, testimony to the Senate Y2K Committee, 7 October 1998.
3. Survey available at http://www.nerc.com/y2k/summaries.html.
4. See NFIB News, "Small firms pick up pace in dealing with Y2K problems" at http://www.nfibonline.com.
5. See http://www.senate.gov/~y2k/documents/report/index.html.
6. See http://www.y2k.ca.
7. See the 16 March 1999 news report at http://www.sightings.com/ufo/y2khire.htm.
8. R. MacMillan, "Oil and gas industries in high octane Y2K mode," 18 February 1999, at http://cnnfn.com.
9. 31 March 1999 survey results are available at http://www.aha.org.
10. See http://www.fda.gov/cdrh/yr2000/year2000.html.
11. Network Group, "Year 2000 Problem Status Report" to the National Security Telecommunications Advisory Committee, September 1998. Available at http://www.ncs.gov/n5_hp/Customer_Service/NCS-Y2K/Year2000a.html.
12. J. C. Willemson, testimony before the Subcommittee on Technology, U.S. House of Representatives, 6 August 1998 (report GAO/T-AIMD-98-251, U.S. General Accounting Office, Washington, DC).
13. J. Jinnett, "Legal issues concerning the year 2000 computer problem: an awareness article for the private sector," available at the Law Center of http://www.year2000.com.
14. See http://www.y2k.gov.
15. See http://www.fema.gov/y2k/ccmp.htm.
16. For the United Nations, see http://www.un.org/members/yr2000; for the World Bank, see http://www.worldbank.org/infodev/y2k; for the European Commission, see http://www.ispo.cec.be/y2keuro/year 2000.htm.