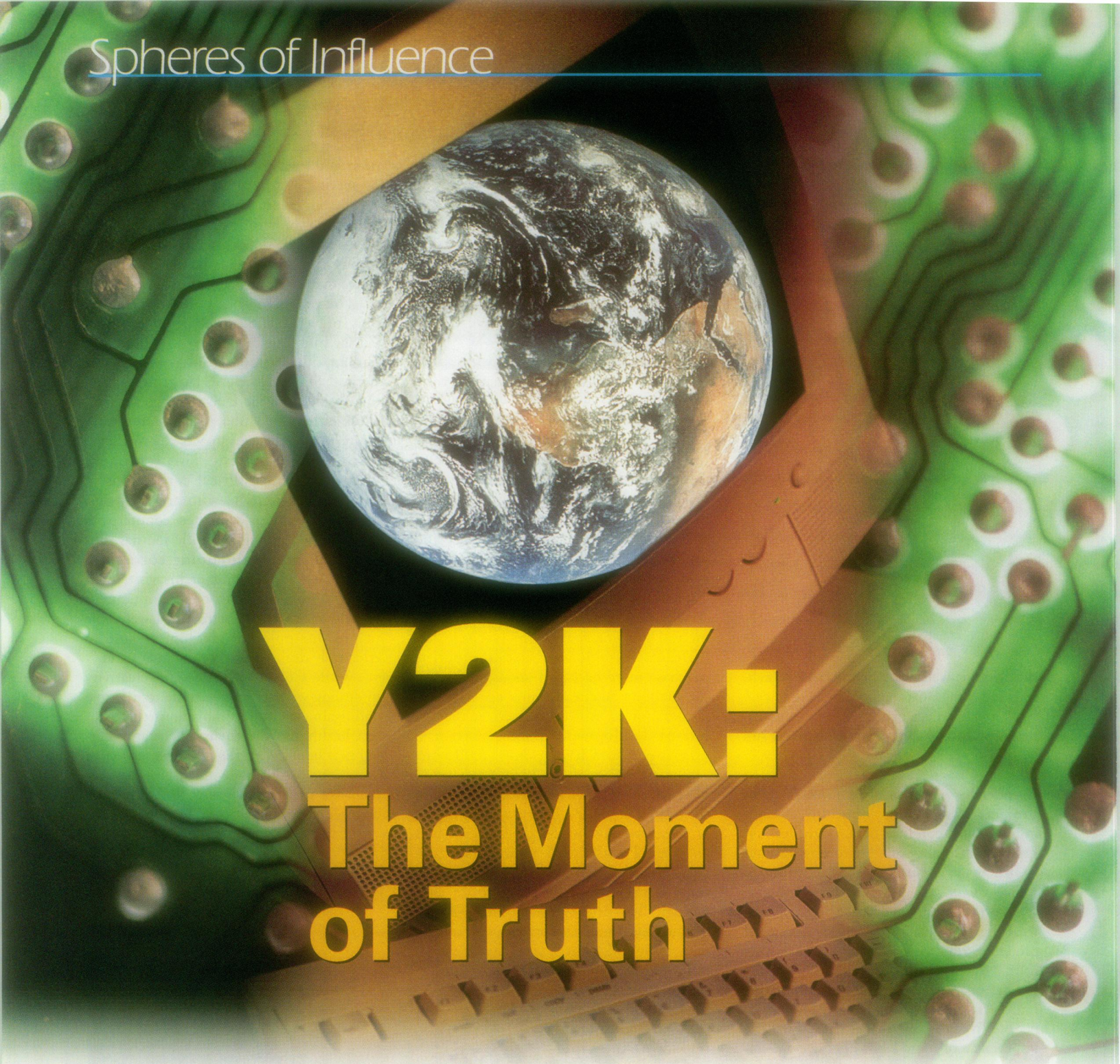

Y2K: The Moment of Truth

Scenario one: The year 2000 has arrived, but the world is in no mood to celebrate, for the two-digit nightmare that pundits have been predicting has come to pass. Computer systems everywhere are misreading the "-00" in the date and shutting down certain functions, resulting in a multitude of problems. Explosions are occurring at chemical plants in several developing countries because valves are sticking and feeding an oversupply of the chemicals for mixing. Oil from rigs in the North Sea is spilling into the water and polluting the environment after valves begin malfunctioning and keeping the oil pumping. Closer to home, hospital elevators in many U.S. cities are stalling between floors, stranding patients and hospital caregivers. Meanwhile, at government agencies, officials trying to sort records by date are reaching an impasse. And these are just a few of the complications resulting from the so-called Y2K bug.

Scenario two: On New Year's Day 2000, the world breathes a sigh of relief, for there have been only minor computer glitches as a result of the Y2K bug. Sure, there have been power outages in certain parts of the world, and a few industrial facilities have unintentionally released potentially dangerous chemicals into the environment, but the electrical power grids that serve the United States are still functioning and have experienced only minor problems. Moreover, for the most part, the computerized timers at chemical plants haven't malfunctioned, and municipal incinerators are burning waste at the right temperature to destroy dioxins and other carcinogens. Most importantly, though, Russia has had no nuclear accident.

Which scenario will prevail, come the year 2000? It remains to be seen whether the world will move in time to fix the Y2K bug—which has been described as the

biggest single information project the world has ever seen—or whether chaos will reign as computers around the world shut down when the clock strikes midnight on 31 December 1999. "No one knows for sure what will happen, but the year 2000 problem can affect anybody or any entity dependent on computers, and even those that aren't," says Minda Zetlin, the author of *Computer Time Bomb: How to Keep the Century Date from Killing Your Company.*

Alistair Maughan, a partner in the London-based law firm Shaw, Pittman, Potts, and Trowbridge, which advises clients on a full range of environmental issues, says it's clear that Y2K could have a serious impact on environmental facilities, particularly given the extent to which computer software and microchips are now involved in pollution control and environmental monitoring and protection systems. "These systems are just as much at risk as other systems, although the consequences of failure to ensure year 2000 operation may be greater than for other systems and, in certain circumstances, may be potentially disastrous," Maughan says.

A Shortcut Gone Awry

The groundwork for the Y2K problem was laid 30 years ago at the dawn of the computer age, when programmers weren't thinking much about the next century. To facilitate their work and to save computer memory, programmers used just the last two digits of the year for dates (for example, "68" for 1968). The new millennium and its accompanying rollover was three decades off, and the programmers believed there was no way their code would be in use then. The problem now arises that on 1 January 2000, computers may fail to recognize "00" as an actual value and may get stuck in an endless loop, searching for a viable value. Alternatively, they may recognize the date as "1 January 1900."

"Flawed designs became the standard throughout all sectors of the world community," explains Gerald Poje, a member of the Chemical Safety and Hazard Investigation Board and a specialist in both toxicology and policies dealing with chemical hazards. "Large technology systems developed around failed computer designs, thereby creating a monumental problem," he says. These failed computer designs permeate environmental operations and facilities. Treatment plants, refineries, and power generating units, for example, depend on computerized systems for environmental control, reporting, and monitoring, as well as so-called "fail-safe" modes that are supposed to halt operations when serious problems occur. Embedded microcomputer chips are found in such vital operations as alarm, cooling, and heating systems of nuclear power plants, electric utility power lines and plants, and drinking water and wastewater treatment plants. Failures of these systems could have dramatic effects on public health. As the American Water Works Association noted in a recent report on its Web site, "Even a very small water system that is using just one or two [personal computers] is likely to be overwhelmed by the number of embedded computer chips that may be found in the system."

Of the 4.7 billion computer chips produced worldwide in 1997, 4.6 billion went into embedded systems, says Poje. Of these, only 1–3% are likely to have Y2K problems, and only a tiny number of those are in so-called "mission critical" systems. Mission critical systems are those systems vital to an organization or entity's functioning. There are an estimated 50 billion embedded chips worldwide, however, and of those a potential 25 million mission critical systems containing embedded chips could have a date problem. "Each of these chips and the system within which they operate have to be individually tested, but finding them has been a serious problem," says Poje.

Much of the Y2K attention has been directed at the potential impact on the financial and business sectors. But the world community has recently begun to recognize that Y2K could result in serious environmental health and safety hazards, given that date-related computer failures can lead to sewage backup, polluted drinking water, unsafe landfills and incinerators, and interruptions in the power supply.

Computer and computer chip failures relating to the incorrect processing of dates is not a hypothetical scenario, warn some people familiar with the Y2K issue. "Already, a number of date-related failures have occurred," says Lois Epstein, a senior engineer at the Environmental Defense Fund in New York. "For example, when computers failed to recognize 1996 as a leap year, some industrial damage occurred before the situation could be corrected." For instance, at midnight on 31 October 1996, at an aluminum smelter in Tawai, New Zealand, 660 process control computers hung up simultaneously due to a leap year clocking miscalculation, causing all the smelting potline (electrolytic cells) process control computers to stop working without warning. Without temperature regulation, four cells overheated and were destroyed, and had to be replaced at a cost of more than one million New Zealand dollars. (The year 2000 also happens to be a leap year.)

These examples show that it's not just the stroke of midnight on 31 December 1999 that has the potential to knock out mission critical environmental systems. Other Y2K-related dates of concern include July 1 (the start of Fiscal Year 2000 for 46 states), 21 August 1999 (a global positioning system rollover), 9 September 1999 (a default number that programs use to perform self-diagnostics), and 29 February 2000 (a valid date but a leap year problem).

How Close to a Fix?

The year 2000 is just a few months away, but many countries have barely addressed the Y2K issue. It's probably too late now for many countries to adequately prepare for Y2K problems, says Erik Olsen, a senior attorney with the New York-based Natural Resources Defense Council, an environmental advocacy group. "A lot of countries, especially those in the Third World, have been doing virtually nothing, so we should be really concerned about what's going to happen overseas," he says.

A World Bank survey released in January 1999 showed that of 139 developing countries, only 15% are taking concrete measures to fix Y2K problems, while 24% are aware of the problem but are not taking action. This inaction could have important environmental health implications. "There are concerns that many countries might have trouble providing adequate food, electricity, and health care after year 2000," says Tim O'Brien, the assistant director for government affairs at the Washington, DC-based Hazardous Waste Action Coalition.

Western governments are worried, too, that Russia's Soviet-era computers, which control nuclear weapons and reactors, will cause problems. Estimates now put the cost of fixing computer mission critical systems in Russia's nuclear arsenal at $3 billion, but the country is strapped for cash and its economy is teetering near collapse. "The U.S. government is concerned and is monitoring the Russian nuclear situation closely," says Gary Purdy, a health physicist with the Nuclear Regulatory Commission (NRC). A 2 March 1999 National Public Radio report stated that Russian officials are playing down any threat of a nuclear accident as a result of Y2K, even though Russian officials have allocated only $4 million dollars to reprogramming the computers responsible for nuclear missile launching.

In the United States, the lack of preparedness is posing a formidable challenge

to environmental protection and public health as the year 2000 approaches. Half of all county governments lack a plan to deal with Y2K preparedness, emergency response, and contingency planning, according to a survey conducted by the National Association of Counties that was published on 9 December 1998. "This [situation] will impact on the availability of emergency response services, 911 communications, and sewer and water treatment systems," warns Joseph Hughes, director of worker education and training for the Division of Extramural Research and Training at the NIEHS.

A report released in September 1998 by the Oil and Gas Working Group of the President's Y2K Council showed that less than 20% of the 638 oil and gas companies surveyed have included an environmental safety and health component in their current Y2K assessment and remediation plan, and less than 10% have completed their Y2K contingency planning with respect to environmental monitoring and control.

The small- and medium-sized companies in the chemical industry face the biggest challenge in preparing for Y2K, according to participants at a Chemical Safety and Hazard Investigation Board conference held in December 1998 in Washington, DC. "Those companies are a major concern because they may be less aware of Y2K and have fewer financial resources to develop mitigation plans," says Poje, who adds that the problem is compounded by the fact that 70–90% of the chemical industry's inventory, assessment, and remediation must be directed toward embedded systems.

Most every sector of society is keeping a wary eye on the electric utility and nuclear power industries, and worrying whether they will be fully prepared to meet the millennium bug challenge. "We can't rule out widespread electric grid instability and blackouts," Epstein says. "Remember that nuclear power reactors require large amounts of electricity for essential cooling."

Officials in the electric utility industry have worked hard to ease public concern about the Y2K issue. In January, Robert Hedlund, director of information technology resources at Consolidated Edison, told the press, "We are comfortable where we are right now. Most of our programs are ahead of schedule."

A 1998 study of the electric utility industry by the Electric Power Research Institute, a research consortium based in Palo Alto, California, found that 94% of the United States' electric utilities expect to achieve overall readiness or transition to year 2000 by 30 June 1999, the target date recommended by the North American Electric Reliability Council, an industry watchdog organization. That sounds reassuring, but sources say they are worried about the interconnectedness of the electric supply and the power grids that carry it. A massive grid links North America's electric power plants, spanning the southern part of Canada and stretching across the 48 states of the continental United States and into northern Mexico. The grid is divided into four regions known as interconnections, each of which consists of a tightly meshed system of consumers, transmission lines, and generating stations. "All it would take is to have a problem with a generating or transmission system in one area and a whole interconnection could be knocked out," Olsen says.

There has also been concern that power outages may have other potentially devastating consequences, for instance, by causing untreated water to be released at water treatment plants, thereby contaminating drinking water supplies. At hearings before the Committee on Transportation and Infrastructure of the U.S. House of Representatives on Y2K Compliance by large drinking water suppliers, John Carman, water quality manager of the Metropolitan Water District of Salt Lake City, Utah, said, "We are concerned about the potential external impacts of problems with the power supply. For example, there are several sewage lift stations operating in our watershed. If the lift stations are offline for a few hours, sewage overflows can contaminate our raw water supply."

Corman said that the Metropolitan Water District of Salt Lake City serves an estimated population of 325,000 people, but that its water has the potential to reach as many as one million people at some point during the year. In all, the U.S. population of 247 million people is served by 55,427 community water systems, according to the American Water Works Association.

Since 1996, the NRC has been working with nuclear power plant licensees and the Nuclear Energy Institute, a nuclear industry organization, to ensure that plant systems are ready for the year 2000. In May 1998, the NRC notified all utilities operating nuclear plants that they had to inform the federal agency of steps they are taking to see that computer systems will function properly by the year 2000.

"The NRC believes it has the Y2K situation under control," Purdy says. "We have done assessments and haven't found any health and safety issues. Besides, most nuclear safety plant systems are operated and controlled by analog equipment that is not date-dependent or vulnerable to Y2K problems." The NRC, however, has found problems in computer-based applications such as security computers, radiation monitoring, and emergency response systems. Purdy believes this is not a problem because, he says, nuclear reactors can be shut down manually in a matter of hours.

Unlike the nuclear power industry, the health care industry is far behind in its Y2K compliance efforts. The Gartner Group, a Stamford, Connecticut-based research organization that is monitoring the Y2K situation, reports that seven out of eight health care groups risk major failures of their systems because of their insufficient response to the Y2K challenge. "It's really a question of money," says Mike Paskavitz, president of the Health Care Safety Institute, a health care monitoring group in Beverly, Massachusetts. "Many of the hospitals are cash-strapped. Besides, even the biggest hospitals have small information technology staff and budgets."

Checking a system for Y2K problems and making improvements can be a formidable task. At just one hospital, for example—the John C. Lincoln Hospital in Phoenix, Arizona—600 personal computers, 6 mainframe computers, and 1,400 biomedical and facility management devices including everything from elevators to heart monitors must be tested. The cost for assessing Y2K compliance of network equipment, desktop computers, and servers for just for one hospital system—the University of Pennsylvania Health System—is estimated to be $1 million. Health care providers are moving to share test results and costs.

The Costs of Compliance

The so-called "Big Fix" for the Y2K problem is expected to cost hundreds of billions of dollars. The money being spent by governments, organizations, and corporations to become Y2K-compliant is staggering. For example, compliance figures are estimated at $4 billion for the U.S. government, $187 million for the State of California, $500 million for the Federal Express Corporation, $550 million for the Bank of America, and $540 million for American Express.

The federal government has reported that it will spend $15 million to keep the old Rocky Flats nuclear weapons plant's computerized electronic devices from failing. Some of the devices trigger alarms if a building's air is contaminated with

radioactivity, while others control the security systems protecting weapons-grade plutonium stored at the site.

The Electric Power Research Institute speculates that the top 300 North American power-producing facilities will ultimately spend the same amount to inventory and test embedded computer systems for Y2K problems as the remaining 300 small electric utilities. The total projected Y2K compliance bill for the U.S. electric power industry is $600 million.

The EPA has launched an outreach program aimed at industry and state and local regulators that promotes the resolution of Y2K environmental issues while explaining the results of failing to do so. In the words of an EPA statement, "Facilities have a responsibility to take whatever steps are necessary and appropriate to assure the accuracy of information and data required to the U.S. EPA and state programs."

Under a policy adopted 30 November 1998 and updated in the 10 March 1999 *Federal Register*, the EPA's Office of Enforcement and Compliance Assurance is waiving civil penalties and recommending against criminal prosecution for violations of EPA rules that result from efforts to test for and eliminate Y2K problems. According to the policy, waivers are "limited to testing-related violations disclosed to EPA by February 1, 2000, and are subject to certain conditions, such as the need to design and conduct the tests well in advance of the dates in question, the need to conduct the tests for the shortest possible period of time necessary, the need to correct any testing-related violations immediately, and other conditions to ensure that protection of human health and the environment is not compromised."

For violations occurring after 1 January 2000, the EPA will recognize a facility's "good faith efforts" in determining appropriate penalties for violations. "Qualifying for the waiver will depend largely on an enterprise's ability to demonstrate that it used all reasonable efforts to solve problems in a timely fashion and avoid or lessen adverse effects," explains Gary A. Jonesi, senior counsel for strategic litigation at the EPA's Office of Regulatory Enforcement in Washington, DC.

Of the state of Y2K compliance in the United States, Jonesi says, "Because no one has yet taken advantage of the policy and we're not aware of any Y2K-related environmental violations, we don't think the year 2000 issue will pose a major environmental problem. The concern, though, is that while larger companies and municipalities are doing a pretty good job, one has to begin to wonder about isolated companies and localities on the smaller scale of things," he says.

Web Sites on Y2K and the Environment

U.S. EPA Y2K Web Site
http://www.epa.gov/year2000

Hazardous Waste Cleanup Information Web Site
http://www.clu-in.org/y2k.htm

Year 2000 Information Center
http://www.year2000.com

U.S. Chemical Safety and Hazard Investigation Board
http://www.chemsafety.gov

Environmental Defense Fund
http://www.edf.org

American Water Works Association
http://www.awwa.org

North American Electric Reliability Council
http://www.nerc.com

President's Council on Year 2000 Conversion
http://www.y2k.gov

The costs of Y2K noncompliance could include legal bills as well. Lawsuits will inevitably result from breaches of contract, personal injuries, and business and organizational interruptions, and could even involve stockholders if the millennium bug hurts business solvency and stock prices.

Lawsuits are already being filed. In January, a doctor named Mario Yu filed a class action lawsuit against IBM and its business partner, Medic Computer Systems, claiming that the two companies were aware that the bundled package comprising IBM's RS/6000 server and version 7.0 of the Medic application software is not Y2K-compliant. The consequences of the Y2K defect, Yu's complaint alleges, could affect thousands of health care providers and disrupt critical systems.

Senators John McCain (R–Arizona) and Slade Gorton (R–Washington) have announced their intention to introduce legislation that would curb unnecessary litigation resulting from Y2K computer disruptions. Lawyers, however, are warning the environmental community not to depend upon government legislation to protect their financial solvency or to keep them out of court.

Enterprises should keep good records and document the steps they take to become Y2K-compliant, legal experts advise. "If you think you are Y2K-ready, something can still go wrong," says James S. Stokes, a partner in the environmental practice group of the Atlanta-based law firm Alston and Bird LLP. "But move to correct the bug and you could be protected legally if you have records showing you made a good faith effort to fix the problem."

Doug Ey, a lawyer in the Charlotte, North Carolina-based law firm of Smith, Helms, Mulliss, and Moore, echoes the point that it's very difficult to guarantee full compliance on the Y2K issue. "I know of companies that have spent millions of dollars correcting the problem," he says, "but during the testing phase, they found other problems."

It is vital, too, that companies dealing with environmental issues have a contingency plan that puts into place mission critical health and safety plans. The American Water Works Association advises companies to assume the worst case scenario for the year 2000 and then ask these questions: what systems are vital, how can these systems be kept in operation, what resources are needed to do so, and how can these resources be made available? They also advise companies to be sure to have enough supplies stored for several weeks of operation without the need for replenishment.

"At this late date, we are advising our clients to focus their energy on prioritizing mission critical systems, and at the same time to put in place disaster recovery plans in the event the unexpected happens," Maughan says. "Given the limited, and now shrinking, resources available to combat Y2K, many organizations and institutions have no choice but to focus on contingencies rather than outright prevention."

Ron Chepesiuk