

April 15, 1999

Y2K: The Millennium Is Now

Focused efforts in the final months can prevent business failures

Today's reliance on computers makes many aspects of life susceptible to the year 2000 (Y2K) bug. The effects can range from minor inconveniences to vital shutdowns. Civilization will not collapse if coffee makers fail to brew or credit-card companies mistakenly charge 99 years of late fees and interest. Lives could be lost, however, if hospital equipment malfunctions or an oil shortage leaves citizens without heat in the middle of winter.

The ubiquity of computers and microprocessors virtually guarantees that every member of civilized society will feel the bite of the millennium bug in one way or another. To mitigate the consequences of the well-publicized glitch, the public and private sectors must cooperate by sharing information with each other and with the general population. Timely, meaningful disclosure can help dispel one of the greatest threats posed by the Y2K bug: fear of the unknown escalating into public panic.

Recent issues of The Lipman Report have addressed both the global impact of the Y2K problem and the domestic impact on U.S. businesses. This issue examines the progress made thus far in addressing the error and offers suggestions to help organizations and individuals prepare for the impending Y2K deadline.

The Millennium Is Now

Even though the new millennium will not technically begin until January 1, 2001, the millennium bug has already arrived. According to a survey by an information technology organization, more than one-third of the 400 respondents reported Y2K problems, ranging from chip failures to computer crashes. Twenty-eight percent had experienced errors with commercial software packages that claimed Y2K compliance. Perhaps the most telling sign of the glitch's arrival is the increase in Y2K-related lawsuits. So far, nearly 80 lawsuits have been filed, with hundreds more to follow. The number of lawsuit demand letters—the step before an actual filing—has skyrocketed to 790 from only 11 in 1998. The first Y2K lawsuit involved a new grocery store whose cash registers and credit card verification machines crashed whenever customers used credit or debit cards that expired in “00.” The owners claimed that frustrated shoppers left and never returned to give

the store a second chance. Most lawsuits, however, involve customers suing vendors that sell products with no Y2K solutions. Y2K vulnerabilities have been identified in a wide range of products, including medical and telecommunications equipment, failures in which could produce loss of life. The U.S. Congress is currently considering several bills to limit liability and help curb the projected tidal wave of Y2K litigation, which some experts estimate could reach as high as \$1 trillion worldwide.

Organizations around the world have already felt the impact of the programming shortcut that reduces years to two digits, causing some computers to interpret the year 2000 as 1900. While some problems occurred during rollover simulations, others resulted from lesser-known trigger dates. For example, police computers in three Swedish airports failed at midnight on January 1, 1999, leaving police officers unable to issue temporary passports or travel documents for several hours. That same day, taximeters in Singapore malfunctioned at noon, halting taxi services for hours as officials scrambled to return the systems on-line.

Time Is Running Out

Many organizations will not complete Y2K repairs before the rollover arrives. Virtually all of the press regarding government agencies' compliance indicates that federal agencies expect to have remediation efforts completed before December 31, 1999. Yet, the report released by the U.S. Senate in February on the nation's progress in addressing the millennium bug crisis indicates that several agencies lag significantly in their compliance efforts. The Senate committee concluded that many companies and agencies in the United States will not complete their compliance efforts in time. The committee also expressed concern over the ability of state and local governments to finish Y2K preparations in time. A national survey of 500 counties revealed that only half of the respondents had countywide plans to

(continued on next page)

Y2K: The Millennium Is Now

Focused efforts in the final months can prevent business failures

(continued from preceding page)

address the millennium bug crisis, and less than one-fourth have contingency plans to deal with potential Y2K disruptions, such as power outages or malfunctioning traffic signals.

While most experts believe that total failure of the national infrastructure is unlikely, the likelihood of local and regional disruptions remains a possibility, especially given the lack of progress at the local levels of government. This situation could be especially dangerous for emergency services. Not only does the millennium glitch threaten to interrupt the ability to process and respond to calls for assistance, but the rollover date of January 1, 2000, could also prompt an enormous increase in the demand for emergency services. A Y2K glitch in the highly automated 911 services could interfere with the ability of ambulance services and the fire and police departments to respond to calls, threatening significant loss of life or property. Such a scenario could trigger a wave of liability litigation, producing substantial jury awards.

Reliance on organizations to report their Y2K remediation progress has yielded dubious assessments for most industries, making it difficult for American businesses to determine their risks. The situation becomes even more grave in light of today's global marketplace. As addressed in the February 1999 issue of *The Lipman Report*, many nations have not committed the necessary time and resources to resolving the millennium bug, which jeopardizes American companies that have. Recent events have demonstrated that today's interdependent economy leaves the United States of America highly vulnerable to economic turmoil elsewhere in the world.

The Y2K Bug Bites Back

As if Y2K failures were not enough cause for concern, organizations are now beginning to worry about the risks associated with repair. In January, for instance, a new billing system installed by a public utility company contained a glitch that overcharged customers whose electrici-

ty and gas usage had to be estimated, with one customer's bill increasing more than sixfold. This event raises an important concern regarding Y2K compliance efforts: the widespread correction of computer code increases the likelihood of disruptions by the introduction of new errors.

This situation creates additional problems for organizations as they attempt to repair the glitch. Not only do businesses need to try to correct all date-sensitive programming that affects mission-critical operations, but they must also develop contingencies against potential failures arising from imperfect repairs. Because the computer industry relies upon humans, bug-ridden "fixes" occur with alarming frequency. Recent studies have uncovered rates as high as 1,200 errors per 100,000 lines of repaired computer code.

To help organizations with their testing, one company is offering to check up to 100,000 lines of Cobol code for Y2K errors at no cost. Several hundred mainframe and minicomputer users worldwide have accepted this offer, submitting the code in which they had the most confidence, and none has been error-free. The best example contained only six critical errors, while the worst had 200. In fact, the company has typically found more Y2K errors in renovated code than in unmodified programs.

Guarding against the Y2K Glitch

Organizations and individuals can still prepare themselves for the impending deluge of Y2K failures. Prompt action is especially critical among small to mid-sized businesses, since many members of this sector lag significantly behind their larger business partners, jeopardizing companies with strong compliance programs. Fortunately, the repairs necessary to solve millennium-bug issues within smaller organizations can often be completed in a relatively short period of time at a small to moderate cost, which means immediate action may yet yield a comprehensive compliance program. To assist smaller businesses in its remediation efforts, the U.S. Congress recently passed the Small

Business Year 2000 Readiness Act, which authorizes the Small Business Administration to guarantee loans to small businesses to repair computer malfunctions stemming from the Y2K glitch.

The following guidelines can help businesses and individuals protect themselves from the millennium glitch in the months to come:

- *Perform a comprehensive inventory and assessment.* For a business or organization, this step involves a systematic evaluation of all computer systems and embedded microprocessors in the facility and elsewhere in the supply chain. This inventory requires identifying and documenting all hardware and software components, including vendor, model, serial number and function. System elements that involve data exchange between programs or partners present a special risk: a non-compliant supplier could unknowingly transmit faulty data that corrupts an internally compliant network.

To help reduce disruption at home, individuals should perform a similar inventory, including household appliances with embedded microchips, as well as the home computer system. Examples of Y2K-prone equipment include fire and security alarm systems, programmable thermostats and garage door openers.

- *Prioritize the repairs needed.* One of the leading Y2K consulting firms predicts that 30 to 50 percent of companies worldwide will suffer at least one mission-critical failure, although that rate drops to 15 percent for American businesses. Such failures are projected to last at least three days, with a recovery cost ranging from \$20,000 and \$3,500,000—excluding litigation costs. Companies need to prioritize vulnerable systems according to their relative impact on business continuity and the organization's financial well-being. Malfunctioning voice mail might prove inconvenient, but the services of a temporary receptionist could alleviate the situation. An inoperative payroll or billing system, however, could bring a company to a permanent halt.

In the household, individuals need to decide which potential malfunctions they can live with. A malfunctioning time/date stamp on the answering machine may be tolerable if the machine still works, but people who track their finances on their home computers will not want to take chances with such information.

- *Execute the remediation plan.* After identifying vulnerable components, organizations need to determine whether it would be more cost-efficient to allow outside consultants or internal staff to implement the compliance program. Outsourcing may offer the only solution to smaller companies without the appropriate human resources, but it presents important security risks. For example, programmers can incorporate back doors into software, which will facilitate future maintenance, but can also provide computer criminals access to the network. In addition, employing contract programmers offers an opportunity for unscrupulous individuals to learn about the inner workings of a network security system. The anticipated chaos from the millennium glitch also presents a possible diversion to enable white-collar criminals—or hackers and terrorists—to perpetrate theft, arson or violent crimes. Proper screening and close supervision of vendors and contract employees can help decrease an organization's security risk.

If a company elects to perform remediation internally, management needs to assign a specific team to the project full-time. Should compliance efforts involve modifying licensed software, however, companies need to contact the vendor before proceeding. Otherwise, the manufacturer could accuse the organization of reverse engineering. Altering a licensed product may also switch liability from the manufacturer to the user, posing yet another risk.

- *Test the plans to ensure effectiveness.* Companies need to begin testing efforts upon completion
(continued on next page)

Y2K: The Millennium Is Now

Focused efforts in the final months can prevent business failures

(continued from preceding page)

ing a repair or installing a new system, rather than waiting until the entire organization has supposedly achieved compliance. Also, the testing phase should analyze how the various systems interact with each other, as well as compliance of individual components. Independent systems that demonstrate compliance may trigger errors elsewhere. The best programs involve coordination with suppliers and vendors to ensure that outside systems do not cause problems with internally compliant systems.

For individuals, compliance testing will focus on the personal computer. Most computer manufacturers post Y2K compliance information on their web sites, as do many software companies. After backing up all critical information, users can manually test system compliance by setting the date ahead to 12/31/1999 and simulating a rollover. In addition, several automated tools are available to assist with the testing process, some of which are free of charge.

- *Develop a contingency plan.* Companies need to define and document Y2K failure scenarios resulting from errors introduced during remediation or from delays in repairing and testing. These scenarios should include potential infrastructure disruptions, as well as possible breakdowns in the supply chain. An in-house task force should develop scenarios and their proposed solutions. This task force also needs to oversee the implementation and testing of the contingency plan. To ensure that the plan addresses all aspects of an organization's operations, the company needs to identify the executives responsible for all key business operations, both internal and those involving the supply chain, and appoint those individuals to the task force. In this manner, senior management can work with the security director and safety and facility managers to develop a comprehensive business continuity initiative.

For household contingency planning, individuals should take basic precautions. Such measures need to include: backing up computer files and maintaining copies of all financial records and statements; keeping small amounts of extra cash on hand; and having extra blankets and cold-weather clothing. Because of potential disruptions in food delivery or errors in water purification systems, some households are considering storing extra supplies of non-perishable food and water. Standard winter-storm precautions can see a family through any inconvenience without fueling the survivalist frenzy that could cause more damage than the millennium bug itself.

The crisis known as the millennium bug has already caused numerous problems worldwide, with countless more to follow in the months ahead. Organizations that began compliance efforts the earliest still have much work to do, and half of small- and medium-sized businesses have yet to address the problem at all. Public and private entities alike need to work together to meet what could prove to be one of the biggest challenges to face the civilized world. Large, well-prepared organizations must assume an active leadership role in encouraging their smaller counterparts. Companies that believe compliance is too expensive need to remember that repairing problems now will cost much less than solving them after disaster has struck.

Although the Y2K deadline lurks only months away, organizations cannot relax in their compliance efforts. Continuous testing can uncover new problems introduced during remediation and help prevent devastating consequences. Even at this late date, a focused compliance initiative during the time remaining can mean the difference between survival and extinction.



The Lipman Report Editors