

March 15, 1999

## The Millennium Bug: Myth or Monster?

The actions of American businesses can determine the severity of the Y2K bug's bite

*With the year 2000 less than 10 months away, virtually every American is aware of the so-called millennium bug, which causes some computers to interpret the year 2000 as 1900. Several years and billions of dollars into the Y2K compliance effort, experts on the subject still do not know what to expect at the year's end. Enough testing has already been completed to indicate that some of the more catastrophic predictions—such as airplanes plunging from the sky and elevators plummeting down their shafts—will probably not come to pass. At the same time, enough blunders have already taken place—such as computerized inventory systems rejecting products that expire in 2000 and beyond—to show that the transition to the new millennium will most likely have a few bumps.*

*Every day the media make new pronouncements about the nation's progress in achieving Y2K compliance. Many organizations, both public and private, have already spent millions of dollars updating and testing internal systems, and their public relations teams have released statements proclaiming their success in exterminating the Y2K bug. At the same time, many other organizations have yet to acknowledge their vulnerability to the millennium glitch, thus jeopardizing those in the previous category. So while much progress has been made, much remains, and American organizations must assess not only their compliance efforts, but also those of their partners.*

*Last month's issue of The Lipman Report examined the global effects of the millennium bug. This edition focuses on the domestic impact of the Y2K bug on U.S. businesses.*

### The Arrival of Y2K

Organizations have less time than they realize to protect themselves against the Y2K glitch, as an East Coast credit union discovered early last month. When the financial institution switched vendors, the millennium bug struck, and 10,000 customers received statements for other people's accounts. Ironically, the credit union had changed vendors to achieve Y2K compliance. Although the problem was corrected the day after it came to light, the case demonstrates that the Y2K bug is not waiting until the Year 2000 to rear its ugly head.

In fact, several organizations have already experienced problems stemming from the Y2K issue. Last summer, the billing system for a Midwestern hospital malfunctioned because it automatically projects 18 months ahead and could not handle the rollover to 2000; the institution could not register patients in the computer for one day. The inventory control system for a retailer refused to accept pharmaceutical products that expired in 2000 and beyond. According to a recent survey released by an international technology consulting firm, 55 percent of the respondents have already experienced a Y2K-related error, and 98 percent expect more such failures in 1999.

While the Y2K bug can strike at any time, some dates—like January 1, 2000—will trigger a deluge of Y2K-related errors. The first day of the new year remains the most obvious deadline for the millennium bug, but it will not be the first to raise an electronic red flag. For instance, July 1, 1999, presents a potential challenge for those organizations that will begin Fiscal Year 2000 on that date. On August 21, 1999, the dating systems for global positioning satellite (GPS) systems will reset themselves to 0000; software that relies on GPS signals for timing will need to convert the reset GPS timing to correspond with the regular calendar. February 29, 2000, also poses a challenge since 2000 is a leap year. In 1996, computerized controls at a manufacturing plant ignored the leap year and shut down vital equipment at the start of the 366th day, producing approximately \$500,000 in damage.

### Not Strictly an Information Systems Issue

Many companies classify the Y2K glitch as purely an automation or technology issue, thus falling under the responsibility of the Information Systems department. Such a limited focus, however, places an organization's business operations at risk because it fails to consider the impact on the supply chain. Even if a company dedicates the necessary resources to ensure internal compli-

(continued on next page)

---

## The Millennium Bug: Myth or Monster?

The actions of American businesses can determine the severity of the Y2K bug's bite

(continued from preceding page)

ance, non-compliance on the part of a critical vendor could still bring business operations to a halt. "The most obvious impact of the Y2K bug is on internal business processes that rely on automated information systems, but peripheral issues such as supply chain should also be considered," says a former agent and information system specialist with the Federal Bureau of Investigation. "In those operations where you depend heavily upon the supply chain, any disruption caused by Y2K bugs has a negative effect on your business. You may cease to operate not because of a problem that you have, but because of a problem that your suppliers have."

In addition to the bug's effects on workstations and servers, companies need to consider its impact on the physical facility, such as the systems that control access, communication and security. On the first Monday of 1999, a brand-new card-access system belonging to an East Coast insurance company locked out half of the organization's employees because it could not process employee access cards that expired in 2000. Millennium glitches that shut down portions of a facility's maintenance operations can compromise the organization's security and safety.

Yet another problem of characterizing the millennium glitch as a technology issue lies in the fact that many small and mid-sized businesses consider themselves too small and low-tech to be affected. According to a study released by a national organization for independent businesses, more than half of all small firms that use computers or date-sensitive microchips have done nothing to protect themselves from the Y2K bug. This widespread inaction among smaller businesses could produce a devastating ripple effect throughout the business community. To guard against such an occurrence, the U.S. Senate has passed legislation that, if approved by the House Committee, would make money available to assist small businesses with Y2K repairs.

### National Impact of Y2K

Even if every system in the United States were to achieve Y2K compliance before the January 1 deadline, the millennium bug would still have far-reaching impact on the nation.

The tremendous amount of resources spent identifying and fixing the Y2K glitch could produce a profoundly negative effect on the U.S. economy on its own. American businesses are spending billions of dollars in essentially unproductive labor—trying to fix a 35- to 40-year-old problem in an effort to maintain current operation levels. Businesses in the investment securities industry, for example, have spent \$5 billion in compliance efforts during the last three years; this figure represents half of the industry's total profits for 1998. Furthermore, the sheer scale of the problem has escalated inflation rates as organizations jockey for the limited number of programmers available to help find and eliminate the elusive Y2K bug. These factors alone, which do not include the effects of potential business interruptions, could hit American consumers hard as businesses attempt to recoup their losses.

To complicate matters further, Y2K failures in other parts of the world could spawn a global recession, as addressed in the February 1999 issue of *The Lipman Report*. Most of the world has neither the resources nor the expertise of the United States of America to address the millennium bug, and the glitch could cause breakdowns in nations like Russia, China and the oil-producing Middle Eastern states. The result could include nuclear reactor malfunctions, mid-winter power outages, and interruptions in world trade and oil shipments, threatening American interests both abroad and at home. For instance, if an American organization received flawed data from a foreign trading partner, it could unknowingly pass corrupt information to its domestic business partners, producing a chain reaction of errors despite comprehensive compliance efforts.

---

These scenarios represent real threats posed by the Y2K bug; however, they appear simply as examples of situations that organizations should protect themselves and develop contingencies against. Taking them too literally only aggravates yet another unknown variable in the Y2K dilemma: public reaction—or overreaction. With respected groups such as the American Red Cross and the U.S. Senate encouraging U.S. citizens to stockpile food, water and cash before the January 1 deadline, some portions of the population have gone overboard and arranged escape at “millennium retreats.” While many of the tactics used in preparing for digital Armageddon will prove harmless, some—such as a run on the stock market—could exacerbate problems caused by the Y2K glitch and hinder the nation’s recovery.

### **Exterminating the Millennium Bug**

Organizations cannot hope to avoid the effects of the millennium glitch entirely, but they can act to lessen its effects on their business operations.

- *Make Y2K compliance a top priority.* Even though the United States leads the world in Y2K compliance efforts, many American companies have still not acted to protect themselves against the millennium bug—a mistake that could prove fatal to between one and seven percent of U.S. businesses, experts predict. Most of the larger companies have already spent millions of dollars toward eradicating the millennium bug, but many of their smaller counterparts have decided to fix Y2K-related problems as they arise. Because of the interdependency of today’s marketplace, this wait-and-see attitude could have severe repercussions throughout the business community, resulting in substantial losses even to better-prepared business partners.

As a measure of self-preservation, larger organizations must assume a leadership role and encourage smaller businesses to join the Y2K effort. Companies need to make it clear to those organizations within their supply

chain that inaction on the Y2K issue is unacceptable. Businesses that think they cannot afford to commit resources to compliance efforts need to analyze their risks and realize that, in fact, they cannot afford to ignore this problem.

- *Learn about the real Y2K issues.* With all the stories on the millennium bug that flood the daily news, people can easily become dulled to the wildly conflicting reports and predictions. Unfortunately, the severity of the Y2K dilemma requires that everyone make a concerted effort to sift through the deluge to discern the real threats from among the hype. Elevators, for instance, are not expected to plunge headlong down their shafts; at the same time, if facility systems are ignored during this critical compliance phase, people could find themselves using the stairs.

Education on the millennium glitch will not only help organizations keep the situation in perspective, but it will also enable businesses to focus their efforts where they are most needed. The sheer size of the problem—analyzing billions of embedded chips and lines of code to find and correct the handful susceptible to the millennium glitch—rules out the possibility of completing the task before time runs out. By knowing which systems are affected, as well as the consequences of their failure, organizations can work with their security directors and facility managers to ensure compliance of the most critical systems, thus mitigating the potential risk, damage and exposure caused by the bug.

- *Address the issue of disclosure.* Under new guidelines adopted by the U.S. Securities Exchange Commission (SEC), public companies can no longer fulfill disclosure obligations with a general statement indicating they are addressing the Y2K issue. Instead, companies must provide an in-depth analysis of past

(continued on next page)

## The Millennium Bug: Myth or Monster?

The actions of American businesses can determine the severity of the Y2K bug's bite

(continued from preceding page)

actions and anticipated measures for the future, which should include contingency plans. In addition, organizations need to maintain a detailed file that documents the information in the SEC disclosure, which can offer protection against potential litigation. The SEC guidelines legally apply to public companies alone, but all companies would do well to follow their example. Timely, informative disclosure can enable organizations to determine potential risks to their supply chain and focus their efforts accordingly.

In addition, following the SEC disclosure guidelines can help companies prepare for the litigation storm expected to break in the year 2000—a legal frenzy projected by some sources to reach \$1 trillion worldwide.

Already, more than 20 Y2K-related lawsuits have been filed, prompting the introduction of controversial legislation that would limit punitive damages for companies that made good-faith efforts at Y2K compliance. Organizations cannot, however, rely on the U.S. government to bail them out of Y2K-related lawsuits; nor can they depend on their insurance policies. Many insurance carriers limit, if not exclude, coverage for damages that result from the millennium glitch. Some carriers offer Y2K coverage, but at an exorbitant price—with premiums costing as much as 85 percent of the coverage. With no guaranteed safety net, companies must redouble their compliance efforts and—literally—prepare for the worst.

- **Prepare for Y2K-related failures.** Many organizations have already experienced failures resulting from the millennium glitch, and a U.S. technology consulting firm predicts that between one-third to one-half of all American businesses will encounter “mission-critical” business interruptions by early 2000. Organizations must assess which systems and devices are critical to business conti-

nity and ensure compliance of those components through comprehensive, focused testing. This evaluation should include facility and security systems, such as environment and access controls.

Meanwhile, an in-house task force needs to develop detailed contingency plans that include non-critical systems, as well as supply-chain interruptions; this team must imagine worst-case scenarios and prepare for them. The task force should include the security director in contingency planning to ensure the facility's safety and security in the event of system failures.

A company that depends highly upon a computerized command center, for example, may find itself vulnerable to opportunistic criminals if the millennium glitch shuts those systems down.

*As far as the Y2K bug is concerned, the millennium is now. New inconveniences occur every day, and experts predict that problems stemming from the millennium glitch will start to become rampant by mid-1999. Many governments and organizations have already spent billions of dollars and hundreds of thousands of hours in compliance efforts, yet much work still remains—with no guarantee that, even if completed, it will indeed defeat the millennium bug.*

*Despite this disturbing fact, American organizations must continue to lead the world charge in overcoming the millennium glitch. Those businesses that have adequately prepared their own systems must assist their counterparts who lag in compliance, lest the unprepared companies drag them down in a colossal domino effect. To avoid this possibility, organizations must devote proper time and resources to contingency planning. No one can hope to escape the bite of the millennium bug altogether, but adequate preparation can help ensure that its effects will not be fatal.*



The Lipman Report Editors