

February 15, 1999

Meeting the Millennium Bug

Businesses Worldwide Must Prepare to Defeat the Y2K Glitch

As clocks around the world struck midnight on January 1, 1999, they did more than herald the start of a new year; they also began a one-year countdown to the much-anticipated arrival of the notorious "millennium bug," a flaw that makes computers interpret the year 2000 as 1900.

During the last few years—and particularly in the last several months—experts from a wide variety of disciplines have forecast a vast range of consequences as a result of the Year 2000, or Y2K, glitch. These prophets have predicted such events as nationwide blackouts, a breakdown in worldwide telecommunication, interruption in air transportation, and an instant global recession. The most pessimistic have even foretold the end of the modern world, prompting some individuals to build shelters stocked with enough food and water to last several years.

Since November 1978, The Lipman Report has provided intelligence on computer security, keeping readers informed on how to protect their information assets from the ever-evolving threat of computer crime. As organizations worldwide prepare to face the greatest computer challenge in history, The Lipman Report offers comprehensive guidelines to help Corporate America ready its defenses in the months ahead. This edition is the first installment of a series that will focus on the Y2K issue and its effects on the world, on the nation and on everyday life.

Birth of a Bug

The Y2K bug dates back to the 1960s and 1970s, when programmers decided to represent dates with six digits: two for the month, two for the day and two for the year. In dropping the first two digits of the year, software engineers realized significant savings by reducing the required amount of digital storage. The American Standard Code for Information Interchange (ASCII) requires eight digits of binary code, or bits, per character. A four-digit year would need 32 bits, while a two-digit year needs only 16. Until fairly recently, computer memory used to cost hundreds of dollars per megabyte—one million bits; now, the same amount of memory costs only a few dollars.

Even though the cost of memory decreased substantially, eliminating the financial need for such shortcuts, the computer industry retained much of

the old code to ensure "backward compatibility," a concept introduced in the 1960s to bring order to the emerging field of computer development. Computer companies recognized that their customers would not purchase new software every model year, so they ensured that each successive model could operate many of the earlier programs. In this manner, many older lines of code managed to find their way into the modern equipment of today.

The Y2K dilemma affects not only conventional computers, but also everyday items ranging from elevators and traffic lights to telephones and toasters, which use embedded systems. These systems contain microprocessor chips that may control a single function, such as opening and closing a valve. Experts estimate that only one to four percent of these embedded systems have date-sensitive functions that will cause them to stop working. With an estimated 3.3 billion embedded chips in use worldwide, however, identifying those few becomes a Herculean task.

The problem with the embedded chips also underscores a primary obstacle in achieving Y2K compliance within a computer network. Only a small proportion of code contains date-sensitive fields, and in most cases, adjusting these date fields is a fairly simple fix. Identifying those few fields within the estimated eight billion lines of code worldwide, however, presents an entirely different problem. To further complicate matters, many of the programmers who wrote those codes have since retired, rendering much of their quirky coding indecipherable to modern programmers.

Global Effects of the Millennium Bug

To date, U.S. organizations have already spent hundreds of millions of dollars in their efforts to achieve Y2K compliance. As would be expected, some have progressed farther with their Y2K plans than others. Even if every system in the United States attained total compliance before the January 1, 2000, deadline, the nation would still suffer sig-

(continued on next page)

Meeting the Millennium Bug

Businesses Worldwide Must Prepare to Defeat the Y2K Glitch

(continued from preceding page)

nificant repercussions as a result of its relationships in the global arena. For an example of the country's integral relationship with foreign nations, one need only look at the response of the U.S. stock market to the financial crises in Asia and Brazil.

To prepare for this digital D-Day, American organizations must first understand the global nature of the Y2K threat so that they can mitigate the effects of the glitch at home.

- *Many countries are behind schedule.* The United States leads the world in the race to become Y2K compliant, yet many American agencies and businesses lag substantially in this effort. This fact does not bode well for progress in the rest of the world, where—in many cases—other matters have taken precedence. Western Europe, for instance, has focused much of its efforts during the past year on the 1999 conversion to the euro. One of four European nations not participating in this time- and resource-consuming project, Great Britain ranks favorably in their Y2K compliance efforts, according to a recent survey cataloging the global risks associated with the Y2K glitch. At the same time, a European consulting firm estimates that approximately 17 percent of British organizations, representing 38 percent of Gross Domestic Product (GDP), will fail to meet the Year 2000 deadline.

In Asia, businesses are preoccupied with surviving the current economic crisis. As the world's electronic leader, Japan uses more embedded microchips than any other nation, placing it at higher risk for Y2K turmoil than the West. Even so, Japanese businesses have only recently started to take notice of the millennium bug.

Although the Japanese banking industry appears to have the situation under control concerning its computer systems at home and abroad, many of the major banks still need to examine their customers' preparations, in addition to scheduling compliance tests. This situation jeopardizes

Japanese financial institutions because of their many clients in East Asia, where many companies have largely ignored the Y2K issue. In fact, at an Asia-wide workshop held last June in Thailand, representatives from China and Nepal said that national awareness was so low that many people in those countries believed the Y2K bug was simply another computer virus.

- *Lack of global disclosure standards will hinder U.S. businesses.* The U.S. Securities and Exchange Commission (SEC) requires public companies to disclose their Y2K compliance efforts, and the Year 2000 Readiness and Disclosure Act offers limited liability protection to those organizations that share their Y2K findings with others. Many other nations, however, do not demand the same level of disclosure, which leaves U.S. organizations unable to assess accurately the readiness level of business partners in these countries. As an additional consideration, some cultures may hesitate in revealing lack of preparation because doing so would result in loss of face. If not dealt with, these two factors could harm the American economy by hiding compliance problems until too late.
 - *The millennium bug will affect global economies.* The scale of the problem makes Y2K compliance efforts astronomically expensive, with estimates for worldwide costs ranging from \$600 billion to \$1 trillion in technological fixes alone. In addition, Y2K-related problems are projected to fuel a litigation storm that may cost up to \$1 trillion more. To date, most companies have succeeded in absorbing the expense associated with Y2K compliance, but as the deadline draws nearer, the cost of compliance increases geometrically. Furthermore, the resources spent on Y2K compliance do not necessarily enhance productivity. While some organizations may realize economic gains through equipment upgrades, many others will simply spend their time and money trying to maintain their current productivity level.
-

As a result, many experts predict that inflation will increase more rapidly than normal, beginning this year, while productivity will decrease.

Some respected economists have forecast that the Y2K problem will spawn a recession to rival the one caused by the Middle East oil crisis in the early 1970s, when the U.S. GDP fell by 3.7 percent. According to this line of thinking, today's economy depends upon information systems as highly that one relied upon Middle Eastern oil. A similar financial toll would devastate the U.S. economy, which produced an estimated \$8.5 trillion in GDP last year. An equivalent percentage decrease would translate into a \$300 billion loss in GDP in the year 2000. Coupled with the financial crises already occurring in Asia and Russia, such a setback would cripple economic systems worldwide.

- *The Y2K glitch could escalate international tensions.* Last November, a nuclear disarmament group warned that the Y2K bug could lead early-warning systems to malfunction or even trigger the launch of a nuclear missile. Other experts assert that computer-controlled weapons systems are more likely to shut themselves off than to turn on. Even this scenario concerns U.S. leaders as they consider the ensuing escalation of tension should foreign defense systems cease operation. To avert this problem, U.S. officials have started working with the world's nuclear powers to ensure constant communication during the potentially uncertain period. The U.S. intelligence community has also begun to monitor those nations that deny possessing nuclear capability, as well as those hostile toward the United States. International tension could also increase as a result of some airlines' announcements that they would suspend flying to areas considered at high risk for Y2K failures.

A Plan of Action

To protect their interests both at home and abroad, U.S. organizations may want to take the following

steps to help ensure domestic business continuity in the global marketplace after the Y2K deadline.

- *Make a public commitment to Y2K compliance.* Public and private organizations need to announce their commitment to the Y2K challenge. Such a declaration will help emphasize the importance of the issue and can serve as a wake-up call to those governments and businesses that have not yet addressed the problem. As a follow-up to this commitment, organizations should also publish periodic progress reports on their compliance efforts. This constant flow of communication can accomplish two goals: It can challenge and encourage other groups in their respective compliance efforts, and it may also help protect a company against potential litigation by documenting a concerted effort toward Y2K compliance.
- *Assess global risk exposure.* Governments and business organizations need to evaluate their computer operations to determine which systems interact with outside computers, thus exposing internal systems to potential non-compliance problems. A computer that mistakes '00 for 1900 instead of 2000 can easily corrupt the data in another company's system that identifies 2000 correctly. Once an organization has identified these potential vulnerabilities, it can work with those partners to solve compliance issues.
- *Require Y2K disclosure from international business partners.* American organizations need to ask critical questions regarding the Y2K compliance efforts of their partners abroad, and they must obtain accurate, reliable answers. According to the SEC, material disclosure addresses four areas: an organization's state of readiness, the costs of Y2K compliance, associated risks and business continuity plans. Lack of disclosure requirements has made investing in parts of Asia an act of faith since investors cannot assess companies' progress in

(continued on next page)

Meeting the Millennium Bug

Businesses Worldwide Must Prepare to Defeat the Y2K Glitch

(continued from preceding page)

their compliance efforts. To encourage Y2K disclosure, last December the Australian government announced its intention to enact "Good Samaritan" legislation that would parallel the Readiness and Disclosure Act in the United States. The new law, which is expected to pass in early 1999, would offer limited liability protection to businesses and individuals for Y2K disclosure statements made in good faith.

- *Cooperate on a global scale.* Many countries have neither the financial resources nor the knowledge base to address the Y2K issue. As mentioned above, businesses in those nations experiencing economic crises are focusing on their immediate economic needs and largely ignoring the prospective problems associated with the millennium bug. Furthermore, most of the literature on the Y2K dilemma is written in English, placing many of the same countries at an even bigger disadvantage. The interdependence of today's global marketplace does not allow Y2K-compliant nations to ignore their less-prepared counterparts. Instead, those nations leading the Y2K fight need to assist the countries that lag in compliance efforts.
- *Develop a contingency plan.* The United States and other nations that have gained a head start in the race for Y2K compliance cannot isolate themselves from the rest of the world, but neither can they naively hope that their international partners will catch up before it is too late. U.S. government and businesses need to develop contingency plans to allow business continuity amidst potential Y2K chaos. Such plans should include finding alternative suppliers and partners for those functions that rely upon foreign entities. Organizations need to predict specific disaster scenarios and to develop detailed instructions on how to handle each one. Already, several companies have experienced Y2K-related problems, ranging from rejection of credit cards with an expiration date beyond 2000 to the shutdown of a

security system at a Midwest manufacturing plant during a compliance test.

Contingency plans should include the roles of security personnel, who will hold the responsibility of maintaining order and resolving problems. Some systems will fail as a result of the Y2K bug. When the clock strikes midnight on January 1, 2000, organizations need to have complete confidence in their business continuity plans. Adequate Y2K risk assessment and contingency planning could be the difference between survival and bankruptcy.

Because the task at hand is a monumental one, some countries around the globe have joined forces in their efforts to prepare for the unknown events of the year 2000. As the world leader in the Y2K battle, the United States needs to assist other nations in their respective compliance efforts. The global nature of today's economy mandates that the failure of one sector has the potential to devastate the whole. At the same time, U.S. organizations must act in a way that balances the urgency of compliance with respect for the cultural needs of their international partners.

Due to lack of disclosure and lack of historic precedent, no one knows for certain what will happen when the year 2000 arrives. In the best-case scenario, the most widely hyped deadline for the Y2K bug will pass uneventfully, and the world will laugh together at the biggest "non-event" of the millennium. Unfortunately, enough Y2K blunders have already occurred to convince experts that such a tranquil resolution will not come to pass. Organizations around the world must finish—and in too many cases, begin—their preparations to greet the new year. The year 2000 will arrive, regardless of the world's state of preparedness, and we will all share in the consequences.



The Lipman Report Editors