

# **COPING WITH AN ERROR IN A KNOWLEDGE SOCIETY: THE CASE OF THE YEAR 2000 COMPUTER CRISIS**

Stuart A. Umpleby  
Research Program in Social and Organizational Learning  
The George Washington University  
Washington, DC 20052 USA  
Email: [umpleby@gwu.edu](mailto:umpleby@gwu.edu)

## **Abstract**

Correcting the year 2000 computer problem became the largest technical project in human history. It was the largest management challenge since World War II and the largest example of peacetime cooperation in history. The year 2000 computer problem can be thought of as the first large problem of a knowledge society. In January people who had been following the subject were genuinely surprised that the century date change had occurred so smoothly. This paper will answer several questions: What actually happened January 1? Was there really a problem? Why was there so little disruption? Why were there no problems in countries that seemed to be less prepared, such as Italy? Why were there concerns about Russia? Why were Americans not evacuated from foreign countries thought to be most at risk? Finally, the paper will consider what has been learned from the y2k experience that may be helpful in the future.

Key words: year 2000 crisis, knowledge society

## **Introduction**

Virtually all programmers knew that using two digits to represent years would lead to difficulties in the year 2000. Nevertheless, repairs in most cases were postponed until the late 1990s. If equipment had not been repaired, world trade and the global economy could have been seriously disrupted. Many people might have died as a result of chemical or nuclear spills or the failure of urban infrastructure. Several reports have now appeared describing what happened in the days after January 1, 2000 (Clarke and Murphy, 2000; McConnell, 2000; Koskinen, 2000). What can we learn from the year 2000 computer crisis about the management of knowledge societies (Mueller, 2000)?

Until recently, human beings had to cope with two kinds of threats – natural disasters and deliberate man-made disasters. Natural disasters included floods, earthquakes, tornadoes, hurricanes, and diseases. Deliberate man-made disasters included wars, invasions, genocide, repressive governments, and torture. However, as our ability to modify our environment has improved, we are now increasingly threatened by errors, oversights, and unintended consequences. Of course, one could say that poorly designed buildings or lax enforcement of building codes have claimed lives for hundreds of years. But we now live in a global society. Technologies spread quickly around the world. Virtually every major city now uses electricity, telephones, and

fossil fuels. Much of this equipment is automated, and, hence, at least potentially was threatened by year 2000 problems.

In late January Y2K program managers from government departments, large corporations, and international organizations came together to discuss what had happened in early January. The conference was jointly sponsored by the Center for Global Security Research at Lawrence Livermore National Laboratory in Livermore, California, and the International Institute for Strategic Studies in London, England.

## **What Happened January 1?**

On New Year's Eve a lot of equipment was shut down. One report was that electric power consumption was only one third of normal. There were some failures of electric power equipment. However, since demand was low, power could be obtained via the power network from other plants. So consumers did not experience power outages.

In order to keep the Information Coordination Center from being overwhelmed with reports of minor failures, a criterion was established for "reportable failures." Because of quick fixes there were very few failures that met the criterion of "reportable failures." The most affected equipment in descending order of frequency of failure were PCs, servers, mainframes, networks, the internet, security systems, and embedded systems. Among failures, 80% were considered to be insignificant; 16% caused brief service interruptions; and 4% caused significant service interruptions.

Given the small number of glitches reported and the virtual absence of significant disruptions anywhere in the world, one could reasonably ask whether there was a y2k problem. Several replies are usually given to this question. First, knowledgeable executives spent a lot of money to fix equipment. Estimates are that \$500 billion was spent worldwide, that \$100 billion was spent in the U.S., and that almost \$10 billion was spent by the U.S. government. Second, people point to equipment which did in fact fail and note that if repairs had not been made, there would have been many more failures.

Several statements made at the conference illustrate the concerns that people had. Joe Weiss from the Electric Power Research Institute was asked by a rather annoyed member of the audience, "Why didn't you tell people that the electric power grid would work?" Weiss replied, "We did not know that it would work. We thought it would work. We were fairly confident that it would work. We had done everything we could think of to be sure that it would work. But we were not sure. We might have missed something."

A similar statement was made by John Boggs from the International Aviation Transportation Association. He said, "We were uncertain until the last moment." Ed Hillard from Hewlett-Packard/ Agilent said that HP had purchased 60 iridium telephones to be sure that they could communicate among their various field offices. Apparently the people at HP were uncertain whether the telephone system would work. Finally, command centers were set up by businesses and governments around the world. Uncertainty about what would happen was very high.

## **Why Was There So Little Disruption?**

Many explanations were offered for why there had been so few disruptions. In addition to shutting down equipment, in some cases problems were avoided by switching to manual operation. Furthermore, it turned out that fewer embedded systems were vulnerable to y2k failures than was initially feared. There were only six to eight manufacturers of SCADA systems, which were among the systems of greatest concern. These are load-balancing systems which are used in electric power networks, water distribution networks, gas pipelines, chemical and nuclear plants, and even steel mills.

Once embedded systems were recognized as a danger in 1997, people had to learn about them, find them, determine which ones were vulnerable, and then repair or replace the affected systems. This task was

called “the world’s greatest Easter egg hunt.” Fortunately, those who started this task early made public what they had learned. Hence, those who started late learned from those who started early. They could look for and replace only the vulnerable equipment. This greatly simplified the task.

Although the cost of not fixing the problem was very high – failure of critical equipment, loss of market share or even bankruptcy – the cost of making repairs was small in most cases. The money required to make repairs was usually less than one percent of operating revenues, and often less than half of one percent. In contrast, the cost of converting computer systems to handle the Euro is three to six times more expensive. Once top management became aware of the magnitude of the danger and hence the importance of the project, top management became committed and made the necessary resources available.

Critical sectors, primarily electric power and telecommunications, were addressed first. After these were fixed, attention was given to less critical equipment.

Email and the Internet were widely used to increase awareness and to share technical information, and all presenters agreed that the Internet was crucial to the successful outcome. International associations were used to increase awareness, to provide technical information, and to gather reports on vulnerability and progress.

There is low information technology penetration in much of the world. So, many countries simply did not have much equipment that needed to be repaired or replaced. Repairs were thus made quickly, even though some countries started very late.

For me the greatest surprise at the conference was the news that multi-national corporations had been very active very early in all the countries in which they operated. Large corporations were acting abroad as they were at home. They not only repaired their own equipment, they also worked with their critical suppliers. For example, Shell Oil Company held awareness-building seminars, conducted technical training seminars, and made available information on vulnerable systems.

There was unprecedented cooperation among all affected organizations – businesses, governments, and associations. Y2K was perceived as a common threat. Due to economic interdependencies, people realized that everyone had to be ready in order for anyone to be ready.

## **Why Were There No Problems in Italy and Russia?**

Italy is an example of a country where problems were anticipated. It is an industrially advanced country, which means there is vulnerable equipment, and Italy started late in its attempts to repair its systems. The country did not appoint a y2k coordinator until late 1998. He did not have an office, staff, or budget for several months. The first government-wide meeting on y2k was held in Italy in either August or September of 1999. Yet when the y2k coordinator began checking with key utilities, he was told, “It’s been fixed.” This sequence of events created both concern and then disbelief. People first worried that Italy had learned about y2k much too late to repair vulnerable equipment. Then they thought that it was not possible for Italy to have repaired its equipment so quickly. The explanation seems to be that the multi-national corporations had been working with the utilities and key businesses in Italy in order to be sure that they would function. However, apparently no one bothered to inform the Italian government, which learned about the y2k problem through the United Nations conference for country y2k coordinators in December 1998.

In the spring and summer of 1999, there were concerns about Russia’s readiness. The issues of concern were nuclear missiles, nuclear power plants, electric power production, and natural gas supplies to Europe. Nuclear missiles cannot be launched without human action, either in the U.S. or Russia. There was no possibility that a computer failure would launch a missile. The danger was that a computerized early warning system might fail to function, and a country might launch its missiles, thinking that it was under attack. To be sure that such misunderstandings did not occur, a shared command center in Colorado was established, and the hotlines between the White House and the Kremlin, which had not been y2k compliant, were made compliant.

The greatest concerns centered around nuclear power plants and electric power generation. In the spring of 1999, it was learned that the nuclear reactor monitoring systems in Russia and Ukraine were not y2k compliant. If not repaired, this would necessitate shutting down nuclear reactors. However, when a nuclear reactor is shut down, the reactor core continues to be hot for many months. Electricity is required to circulate cooling water. If the cooling water is not circulated, the water boils off, and the reactor melts down, similar to what happened at Chernobyl. The fossil fuel generating plants did not have the capacity both to provide power to the population and to cool the nuclear reactors. The policy in Russia was that power would be provided first to the nuclear plants and then to the population. This was certainly the correct policy in terms of preventing long-term environmental damage, but it meant that the population would be short of electricity during the winter.

An additional problem was that there were y2k problems with the automatic systems of fossil fuel plants in Russia and Ukraine. However, the plants could be operated manually, and they were. Concerted efforts by U.S. and European organizations working with Russian and Ukrainian engineers and managers led to the repair of essential equipment.

## **The Evacuation Dilemma**

The U.S. Departments of State and Defense faced critical decisions in 1999. Should emergency equipment and supplies be pre-positioned overseas in order to protect American citizens living and working abroad? If supplies should be pre-positioned, where were they needed? Furthermore, should American dependents be evacuated from countries that seemed most at risk? If so, the evacuation of American citizens might lead to social disorder among the local inhabitants and hence to political problems in these countries. In the spring of 1999 U.S. government agencies realized that they needed good information in order to make these decisions.

Eventually, three sources of information were created. First, interagency working groups were formed in each country; that is, in each embassy the representatives from the Departments of State, Defense, Commerce, U.S. AID, and others shared the task of gathering information about the local utility services. Second, in addition to talking with the local providers, they also talked with people in international organizations who were familiar with the local providers of electricity, water, health care, transportation, etc. Third, the embassies questioned multi-national corporations. In the fall of 1999, there came a time when the people engaged in gathering this information realized that multi-national corporations, which were also at risk due to possible loss of services from the same utilities, did not seem to be greatly concerned. When government officials asked people in the corporations for their assessment, they were told that the corporations had been working with the local utilities, which were in good shape. Hence, by November 1999 the US government had reason to believe that there would be very few significant disruptions around the world. The decision was made not to pre-position large amounts of equipment and supplies and not to evacuate American citizens.

Given that the government had information that most equipment had been fixed and that there would be few disruptions, why did this information not get out to the general public? Previously, the government had indicated that, although the electric power grid as a whole would not collapse, local disruptions of power and other utilities could be expected (Bennett, 1999; Koskinen, 1999). When the press was asked why they did not publicize the good news, the answer was, "Good news is no news." The good news did have the effect of preventing the publication of stories about possible disasters, but it was not considered newsworthy to report that disruptions would not happen.

## **Lessons Learned**

There were fewer problems with embedded systems, fewer virus attacks, and less public panic than was expected. Indeed there were fewer problems for customers than usual! Y2K led to a rise in the perceived importance of the IT sector in businesses and government. Organizations created new maps of their business

processes and became more aware of their vulnerabilities to suppliers and to local utilities. Many proclaimed that the IT community rose to the challenge.

Some efforts begun by y2k projects will continue. For example, the Department of Energy will continue to work with Russian and Ukrainian nuclear plants. The Department of Defense has become more aware of its vulnerabilities. Ambassador Percy Mangoaela, head of the UN Informatics Working Group, said that he would try to improve the functioning of UN agencies through greater use of email and the Web.

Y2K was the first crisis of a knowledge society, a crisis created by an error or oversight in man-made equipment. Important lessons have been learned, but the lessons need to be widely shared.

## References

Bennett, R. et al. (1999); Investigating the Year 2000 Problem: The 100 Day Report; U.S. Senate Special Committee on the Year 2000 Technology Problem, September 22, 1999. ([www.senate.gov/~y2k/documents/100dayrpt](http://www.senate.gov/~y2k/documents/100dayrpt))

Clarke, J. and R. Murphy, (2000); The Many Silver Linings of the Year 2000 Challenges; Office of Governmentwide Policy, U.S. General Services Administration, January 2000.

Koskinen, J. (1999); Fourth Summary of Assessment Information; President's Council on Year 2000 Conversion, October 1999. ([www.y2k.gov/new/4thquarterly.html](http://www.y2k.gov/new/4thquarterly.html))

Koskinen, J. (2000); The Journey to Y2K: Final Report of the President's Council on Year 2000 Conversion; March 29, 2000. ([www.y2k.gov](http://www.y2k.gov))

McConnell, B. (2000); Y2K: Starting the Century Right! International Y2K Cooperation Center; February 2000. ([www.iy2kcc.org](http://www.iy2kcc.org))

Mueller, K.L. (2000); Two 'Double Binds' and a 'Double Blindness'; annual meeting of the International Society for the Systems Sciences, Toronto, Canada, July 2000.

[top of this page](#)