Y2K: Starting the Century Right!

Report of the International Y2K Cooperation Center
Washington
February 2000

www.iy2kcc.org

Y2K: Starting the Century Right!
Report of the International Y2K Cooperation Center
February 2000

This report tells the story of the global public-private effort to attack the Y2K problem, as seen through the eyes of the International Y2K Cooperation Center and those of the government officials and their private sector partners in over 170 countries. It is the story of the network that led the transition into the twenty-first century. The report's purpose is to document a uniquely successful experience in international cooperation, and to provide an analytical framework for future research.

National Y2K coordinators were provided the opportunity to review the final draft of this report, along with officials from the principal sector organizations mentioned, and all comments received are reflected. Four independent reviewers reviewed several drafts of the report and provided valuable comments and insights.[1]

The IYCC Steering Committee was heavily involved in reviewing the drafts of the report, and has approved its publication. However, any errors contained in the report are the responsibility of the staff of the International Y2K Cooperation Center.

Summary

At the end of the twentieth century, the year 2000 date change problem[2] (Y2K) threatened computers and digital systems around the world. Left unaddressed, Y2K would have seriously disrupted vital financial, business, health, and government services and could have interrupted electricity and telecommunications. While primary responsibility for addressing Y2K rested with each organization that delivered those services, a unique international cooperative effort was organized to provide mutual assistance among nations. As a result, the world moved into the twenty-first century experiencing only minor Y2K problems. This report is the story of that success.

[1] The independent reviewers were: Olivia Bosch, Senior Research Fellow Center for Global Security Research at Lawrence Livermore National Laboratory (California) and International Institute for Strategic Studies (London); Kees van Hee, Professor of Mathematics & Informatics, Technical University of Eindhoven (Netherlands); Lee M. Tablewski, Senior Research Associate, Dante B. Fascell North-South Center, University of Miami; and, Ernest Wilson, Director, Center for International Development and Conflict Management, University of Maryland. Reviewers' independent assessments of the IYCC's activities appear at Appendix N.

[2] In order to save scarce memory and processing time, many computer programs and digital control systems had been designed to use a two-digit field to denote the year. The Y2K problem stemmed from the fact that many calculations and events that depended on the value of the year field would malfunction upon encountering the value "00" on 1 January 2000.

This summary addresses six questions:
- What were the global risks from Y2K?
- What opportunities did Y2K present?
- What assets were available to tackle the Y2K problem?
- What did the world do?
- What were the results of the global effort?
- What lessons can be learned?

What were the global risks from Y2K?

Because the most critical aspects of Y2K were addressed successfully, the full extent of the threat it posed to everyday life will never be known. However, in the late 1990s a broad consensus developed that Y2K could cause at least four serious problems. First, Y2K failures could cause serious economic and social harm. Computer hardware and software that supported financial processes ranging from global capital flows, to government payrolls and benefits, to small business inventories, were highly vulnerable because of the extensive use of dates in these systems. Y2K-induced errors would have caused many of these systems to stop working entirely. Some systems would work, but produce erroneous results, which could be transmitted to other systems, corrupting their data as well. In addition, because some industrial processes and commercial equipment were controlled by digital microprocessors that contained date functions, Y2K held the potential that critical infrastructures such as electricity, telecommunications, aviation, and health care would be unable to deliver services in a normal manner, further disrupting commerce. Y2K errors in defense warning systems could have caused defense forces to react mistakenly. Had these threats been unchecked, serious economic harm would have occurred on a global basis, along with the potential for humanitarian emergencies or international crisis.

Second, public overreaction to Y2K fears could have caused serious hardships. Fears that supply chains would be disrupted could have caused hoarding of scarce commodities such as pharmaceuticals. Fear that the financial system would not be ready for Y2K could have caused runs on the banks. Emerging economies were particularly vulnerable to the potential panic selling of investments perceived as risky, or to the loss of tourism revenue. In fact, some stockpiling did occur,[3] at least one bank ran out of cash and closed for a day, financial markets did briefly reflect worries about emerging economies' viability in the third quarter of 1999, and millennium tourism was lower than expected in many places. No real panic ensued, however, because people believed correctly that the world was ready for Y2K.

The third risk was political. Widespread Y2K failures or panic lasting for more than a few days could have caused political instability. Indeed, the importance of maintaining public confidence in the Y2K preparations became the principal occupation of the global Y2K team in the last months of 1999.

[3] In the United Stares, for example, year-end wholesale inventory growth and retail food and drug sales strongly exceeded normal levels. *Business Week, 31 Jan 2000.*

Fourth, widespread serious computer problems would likely have reduced public confidence in information technology, slowing growth in that industry and potentially derailing technology-led economic growth worldwide.

In the view of some, there were other potential risks. For example some organizations believed that electrical power generation and distribution systems would actually fail on a national or regional basis, creating serious humanitarian emergencies, particularly in the northern hemisphere. By the end of 1999 there was no consensus on the likelihood and duration of such catastrophic failures.

What opportunities did Y2K present?

Beyond these serious risks, however, Y2K offered a variety of valuable opportunities to organizations. While the full story of Y2K's benefits is yet to be written, it is already clear that many organizations used Y2K to bring their information technology systems and software under control. Most organizations did not have a complete inventory of their systems before Y2K. Many determined that redundant systems could be consolidated or eliminated rather than fixed.

Similarly, organizations used Y2K to understand their dependencies on others. Supply chains were inspected and the reliability of key suppliers and customers were evaluated. National contingency plans were created, tested, and modified. Governments at all levels used the opportunity to understand and connect with both the public and private providers of critical services. In general, Y2K produced a useful pruning and organizing opportunity for both systems and relationships.

Among nations, Y2K presented an opportunity to create and test a new form of organization – the first "virtual" international governmental organization -- to address a global problem. Y2K was seen as a common menace that threatened every country. Economic and security interdependencies meant that no country was an island. The problem's clear-cut nature and unyielding deadline gave clarity and urgency to the work. Sharing of information about workable approaches to the problem and about progress toward readiness became paramount. This environment fostered the creation of an agile but official mechanism to validate and share quality information around the world.

What assets were available to tackle the Y2K problem?

Into this mix of threat and promise the nations sent excellent people, in many cases their best managers, to form what became the global Y2K team. People – the national Y2K coordinators from over 170 countries, and Y2K managers from countless public and private international organizations – made the difference. Dedication, experience, and a problem-solving attitude were the attributes that set the leaders of this effort on a course to success.

The second most important asset was a growing pool of quality information. Sharing of best practices for creating a national Y2K office, for managing the program of

Y2K assessment, repair, and testing, and for preparing and exercising contingency plans cut valuable months off the schedule and dramatically reduced costs in many countries. Powerful code-checking tools, not available in 1998, greatly accelerated fixing and testing in 1999. As time grew short, the ability to pinpoint the most critical areas for attention made a crucial difference in the outcome.

People and information were able to work together effectively because of a third asset, electronic networks. The net permitted almost instantaneous communication across organizational and geographic boundaries without respect to time zones. The world wide web, electronic mail, fax, and phone made rapid consultation and information sharing practical and economical.

Of course, no problem of this scale could be solved without money. Support came from both government and industry. Through the World Bank, the United Nations Development Program, and other multilateral and bilateral aid mechanisms, developed countries provided more than $100 million[4] in direct Y2K project assistance to developing and emerging economies. Y2K-targetted loans from the World Bank added an additional $169 million to the significant national-level resources devoted to the project. These governmental efforts remained modest when compared with the estimated $200 billion spent worldwide by private sector organizations to address Y2K, but they were sufficient to permit governments to address the problem in most of their critical systems, and to lead national and international efforts effectively.

Finally, although good will and money were essential, they would not have been enough if two key international institutions, the United Nations and the World Bank, had not stepped forward to provide leadership. Building on a Y2K outreach program begun by the World Bank's *info*Dev program in 1997, the two organizations called together over 120 countries' official Y2K representatives at the United Nations in December 1998. These national coordinators saw the need for an international coordinating body to pull together burgeoning but disparate efforts to attack the Y2K bug on a global basis. In February 1999 the International Y2K Cooperation Center was created under the auspices of the United Nations Working Group on Informatics, with direct funding provided by the World Bank, in-kind support from several national governments, and the assistance of the World Information Technology Services Alliance. The IYCC was never an official arm of either the U.N. or the Bank. It was nonetheless able to interact directly with national government Y2K representatives under the official color of those two bodies, providing the benefit of official sanction without the potential for damaging delay that more formal status might have created. (For more information see "Resources" at Appendix M.)

What did the world do?

The detailed story of the international Y2K effort, and the IYCC's part in it, is the body of this report. For the purposes of this summary, the IYCC's efforts can be summarized by six elements. The IYCC: gathered and disseminated quality information,

[4] All amounts are in U.S. dollars.

organized dynamic regional and global networks, created a flexible response framework, managed rapidly changing public information, predicted most outcomes correctly, and created a global window into the date change event. Each of these elements had the core purpose of supporting national Y2K programs. In every case the IYCC succeeded only with the help of other nations, organizations, and individuals. The IYCC did not solve the Y2K problem; it made the work of those who were solving it more efficient and effective.

Selected IYCC Activity Measures, December 1998 to January 2000

Gathering and Disseminating Quality Information

- Electronic information bulletins sent to 400+ correspondents in 170+ countries about every 10 days.
- Website with over 3000 pages received over 9 million hits.

Organizing Dynamic Regional and Global Networks

- 45 conferences in eight geographic regions.
- Two U.N-hosted global conferences of national Y2K coordinators (including the largest single-issue conference in U.N. history).
- Five meetings and numerous conference calls of the multilateral IYCC steering committee.
- Regular and extensive electronic and in person joint planning efforts on information sharing and action with 20+ national, regional, and global leadership organizations such as the European Commission and the International Civil Aviation Organization.

Creating a Flexible Response Framework

- A network linking the G8 nations, other donor nations, the United Nations Emergency Response Coordinator, the World Bank, and the International Monetary Fund was poised to assist should serious Y2K disruptions exceed the capacity of individual nations.

Managing Rapidly-Changing Public Information

- 8 news conferences, 33 press releases, and countless interviews produced 6000 citations in the global media.

Predicting Most Outcomes Correctly

- Three reports beginning in September 1999 predicted few, if any, serious disruptions, and no nuclear safety incidents.
- Concerns about medical devices and government services proved accurate.

Creating a Window into the Date Change Event

- 159 countries participated in the Global Status Watch, reporting their Y2K status before and after the date change and greatly reassuring the public that the global Y2K situation was well in hand.

What were the results of the global effort?

The global Y2K team delivered a successful outcome. The Y2K bug produced no serious disruptions of critical services on a national, regional, or global level. In addition, there was no significant panic or overreaction caused by Y2K fears. Minor Y2K glitches were reported by national coordinators (see Appendix C for a recent list) and the media, but these were managed by the organizations that operate the affected systems. Many more glitches probably occurred but did not become public as they were quickly resolved or temporarily fixed.

Ironically, the foremost issue that national Y2K coordinators have had to face has been second guessing by those not directly involved in the Y2K effort. Some are asking if too much money was spent to address the problem. These critics point to the apparent

wide range of expenditures by countries, and note that, irrespective of expenditure, the consequences seem roughly comparable. From this they conclude that less could have been spent to achieve the same results.

Analysis shows that the real range of expenditures is much less than appears. As shown in detail at Appendix D, the "Y2K Spending Index" for 50 countries ranges from $318 in Sweden to $2 in Bulgaria. (The Y2K Spending Index reflects the amount spent on Y2K, adjusted for the number of automated systems in the country.) This difference is likely due to a variety of factors. Countries that are more dependent on computers spent proportionately more to fix them. Some countries' Y2K costs were more visible than others.' In addition, many of the lower spending countries started work later. Over time Y2K tools and know-how became much faster and cheaper, permitting those who started later to accomplish the same amount of work at a lower cost.

What lessons can be learned?

The global Y2K experience created a unique opportunity to learn about how the world works and how international cooperation can be improved. While the lessons to be learned will become more evident over time, 18 lessons across three arenas – strategy, information, and management, are explored in detail at the end of this report.

The seven strategic lessons begin by answering the question, "Why was this degree of international cooperation possible?" Two principal factors, the existence of a common menace and cross-border interdependencies, were key. Y2K menaced every country, creating a motivation to learn from the experience of others. But Y2K was more than a national problem. It would do little good to fix your own systems if someone you depended on for critical supplies or markets was not also ready. The combination of these two factors created mutual interest that promoted cooperation. The remaining strategic lessons strongly suggest that, given the right conditions, the world can successfully organize itself to manage a global problem.

As to information lessons, Y2K clearly demonstrated the power of public information, along with some pitfalls to be avoided in interpreting public and private statements about both risk and readiness. Common to these lessons is the notion that those closest to the situation – in this case the national Y2K coordinators -- are more likely to know what they are talking about than outside pundits and prognosticators.

Finally, Y2K provides the basis for a number of constructive suggestions to organizational managers. Common among these is the demonstration that information and communications technologies are critical to the missions of complex organizations, and that the awareness of technology risks can no longer be the sole province of information systems managers.

Ultimately, the global Y2K experience brings hope that other tough global problems can be solved. Assuring that all the world's citizens can benefit from technology, managing the risks that interconnected technology creates for information

and infrastructures, and finding ways to use those technologies to improve governance are but three areas that bear further exploration and research. As the global Y2K team disperses, it is our hope and intention that the learning live on in other arenas, and that the benefits of Y2K accrue around the world in the decades to come.

Y2K Lessons Learned (for details, see Chapter 10, attached below)

Strategic Lessons

1. A common menace and cross-border interdependencies were keys to success.
2. Networking and information cooperation work.
3. Leapfrogging is good!
4. Infrastructures are both connected and resilient.
5. Leadership is vital, but institutional agility varies.
6. Public-private partnerships can work.
7. Technology can be managed.

Information Lessons

8. Facts build confidence.
9. Value self-reporting.
10. Close is better.
11. Details count.
12. Beware information lag.
13. Information cartels have marginal value.

Management Lessons

14. Explain the program in "plain English."
15. Information and communication technology is mission critical.
16. Know your systems, suppliers and business processes.
17. Manage risks proactively.
18. Prioritize requirements for results.

Chapter 10 – Y2K Lessons Learned

Y2K provided a unique opportunity to learn about how the world works, how technology fits into society, and how international cooperation can help solve global problems. The successes and failures of the Y2K effort provide useful insights into how the world might address future issues. Y2K teaches about strategy, information, and management.

Strategic Lessons

Y2K produced seven lessons about solving international technology problems.

1. A common menace and cross-border interdependencies were keys to success.

Unprecedented international cooperation contributed to the successful outcome. Two attributes of the Y2K problem helped make that cooperation possible. First, Y2K threatened every nation, providing the incentive to share best practices and reduce the total costs of fixing the problem. The unmovable deadline of 1 January 2000 gave gravity to this menace. Second, it would do a country limited good to solve its own problems if a neighbor on whom it depended for critical services or supplies was unable to function because of Y2K failures. The interdependency among nations created interest in providing mutual assistance so that all could succeed.

2. Networking and information cooperation work.

Y2K showed that, given incentives to cooperate, a combination of personal contact supplemented and sustained by electronic information sharing can create a virtual organization that works together successfully to solve a tough problem. A central organizing function, while it need not be large, can be helpful to encourage the open exchange of quality information among members of the network.

3. Leapfrogging is good!

Some nations and organizations started working on Y2K much later than others did, but no significant differences in outcomes are yet apparent. While the reasons for this vary (see the discussion on Y2K costs in Appendix D), a critical factor was that the cost and time to fix the problem decreased rather rapidly. For example, in 1996, cost estimates were $1 to $2 per line of business mainframe software code to make Y2K repairs. (A typical accounting program has hundreds of thousands of lines of code.) The cost was also expected to rise to over $4 per line by 1998 as a shortage of skilled programmers developed. In fact, the cost fell to only a few pennies per line because automated Y2K tools became extremely accurate and efficient at fixing the code. On a more strategic level, when people first started working on Y2K no one knew where in power plants, telephone systems, elevators, or chemical plants, there might be date-sensitive embedded processors with a Y2K problem. As it turned out, serious Y2K risks were confined to a small number of situations. Because of information sharing, the late

starters did not need to repeat the work of those who had tested all the systems before them. (The early starters were those who depended most on technology and who could not afford to take a "wait and see" attitude.) Technology and knowledge advances can permit this kind of beneficial “leapfrogging” in other areas. For example, developing countries are skipping the expense of stringing copper telephone wire into rural areas and moving directly to wireless for voice and basic data communications.

4. Infrastructures are both connected and resilient.

Many expressed concern that local Y2K failures could cascade around the world’s interconnected power, communications, and trade networks. Certainly Y2K taught a great deal about supply chains and interdependencies. The phone and electrical power systems each depend on the other for efficient operation. Company and country contingency plans routinely covered what to do if the power went out or if key supplies were delayed. In fact, where there were Y2K problems in critical infrastructure operations, they were handled by system operators without disrupting service to the public. Infrastructure operators are familiar with having to continue service in the face of technical problems. Y2K contingency planning and testing strengthened that ability, and the Y2K success increased confidence that many critical infrastructures would be able to recover from other kinds of attacks.

5. Leadership is vital, but institutional agility varies.

Leadership by formal institutions, including governments (such as those on the IYCC steering committee) and multilateral institutions (such as the United Nations and the World Bank) was essential to success. In many cases, however, that leadership was demonstrated by a willingness of individuals to move forward in the face of an urgent problem without undue regard for normal, formal channels. Y2K demonstrated the benefits of establishing international communications on a non-political level to accomplish a goal that has global implications, without the red tape that dealing with formal institutions typically entails. While this approach avoided many problems, in some cases formal channels were necessary (for example, to approve the expenditure of funds). Here the ability of institutions to make things happen quickly enough to be relevant varied greatly. Increasingly towards the end of 1999, those involved in Y2K adopted a practice of “pushing on any open door” for help, and not attempting more than once to get help where they encountered less active interest.

6. Public-private partnerships can work.

In many sectors public and private sector organizations worked hand-in-hand to solve the Y2K problem. The partnership in finance between the Joint 2000 Council (national regulators) and Global 2000 (financial institutions) set the tone. In aviation, the ICAO-IATA team produced a glitch-free date change. In these and other cases, private sector resources joined hands with governmental authority and sponsorship to leverage the best qualities of each. The international experience and analogous partnerships inside

many countries showed that, faced with a threat that affected entire industries, private and public interests converged.

7. Technology can be managed.

Perhaps the most reassuring aspect of Y2K is its demonstration that humanity can organize itself across boundaries to manage problems in the technology it has created.

Information Lessons

Y2K taught six lessons about using information to manage projects and keep the public informed.

8. Facts build confidence.

The key to maintaining public confidence was the release of detailed readiness information, including what systems were ready, and what contingency plans had been made to ensure continuing services where systems might not be ready. Bland assurances without enough detail to create a credible story proved inadequate. In some cases, information voids developed. In the absence of quality information, rumors and self-serving predictions of doom filled the voids. Countries learned by painful experience the cost in time and frustration of reversing the public view of their readiness status when they had not put information on the record in advance.

9. Value self-reporting.

Almost invariably the outcome predictions of national Y2K coordinators were more accurate than those of external organizations. Many external bodies discounted national coordinators' statements of readiness as self-serving, arguing that the coordinators were telling the best story possible in order to prevent public reaction. In fact, most coordinators recognized that the consequences of making overly positive predictions were far greater than making cautious statements. Coordinators would be held accountable for Y2K results, and a misled public would react more unpredictably than one that had been prepared. Thus coordinators tended to err on the side of caution in their pronouncements, behavior that many external predictors failed to recognize.

10. Close is better.

A corollary to the value of self-reporting was the reliability of sources close to the problem. As noted in Chapter 3, concern by some about Russian natural gas supplies was publicly and accurately dismissed by the Finnish gas company, which was completely dependent on Russian gas. The Finns' close proximity to the potential problem gave them a superior vantage point.

11. Details count.

A frustrating aspect of much Y2K information was its generality. The importance of facts to substantiate readiness claims was noted above. Equally important were the details about the actual effect of potential Y2K "failures." Perhaps one explanation of the often dire public predictions by those without direct responsibility for solving the problem was a lack of knowledge about actual consequences. Certainly many financial and business systems would have stopped operating completely had Y2K repairs been ignored. With respect to equipment with embedded processors, however, which dominated concern about many countries' core electricity and telecommunications infrastructures, Y2K "failure" often meant a lack of correct management information, not service interruption. Too often the crucial question -- "So what?" -- did not get asked about statements that systems were not Y2K ready.

12. Beware information lag.

Information takes time to become public. The normal processes within governments and organizations of gathering data and preparing, summarizing, and checking reports before publication meant that public reports were usually based on status information weeks or even months old. As time grew short, creating reports became less critical than finishing final fixes, adding to the staleness of public information. The final months of 1999 saw most countries meet their predicted schedules, but awareness of this progress lagged among external predictors.

13. Information cartels have marginal value.

Almost every official and private sector Y2K coordinating or evaluating body developed detailed databases containing information about product, system, or country readiness. Most private organizations did not share the details with outside persons for liability, security, or proprietary reasons. These databases ranged from lists of medical devices showing actual Y2K test results to catalogues of airports' sensitive readiness plans. Considerable attention was given to debating the merits of releasing such details to the public. Possession of the details permitted those with access to better focus their Y2K efforts at the specific system level (as with medical devices). At the organizational level (as with airports), the quality of the information usually proved to be no better (and was at times less accurate) than public information.

Management Lessons

Y2K taught five lessons about the management of large-scale projects.

14. Explain the program in "plain English."

Y2K workers around the world learned how to communicate that what appeared to be a technology problem was in fact a business and management problem. They learned how to explain the impact of a technology failure in terms that their organization's leadership could understand. This experience will serve the technology community in the future. At the national level, coordinators learned that, in order to

influence global economic and media organizations, significant attention was needed to ensure that readable English-language versions of their readiness reports reached opinion leaders.

15. Information and communication technology is mission critical.

Management at all levels learned how dependent their organizations are on information and communications technology. For many organizations, their internal systems, those of their suppliers and customers, and the infrastructure itself were at some risk from Y2K.

16. Know your systems, suppliers, and business processes.

Y2K induced organizations to produce comprehensive inventories of their critical systems, and those systems' functions and interconnections. For many organizations this was the first time such inventories were created. At the national level, many countries used Y2K to improve the coordination of emergency response mechanisms. Similarly, organizations emerged from the Y2K effort with a much greater understanding about who they depend on for critical supplies of goods and services. Nations as well learned much about where critical materials and support services come from. Finally, knowledge about systems and suppliers fed into a broader understanding within organizations about the need to know how the organization actually performs its missions. Y2K revealed many intricate processes that had developed over the passage of years, and provided the opportunity to understand and even improve them.

17. Manage risks proactively.

Y2K taught the usefulness of preparing for service interruptions, and the importance of testing, not simply producing, contingency plans. It also underscored the advantage of communicating with the public early and often about matters of potential widespread concern, rather than wait for concern to develop and attempt to correct it reactively.

18. Prioritize requirements for results.

Ultimately what counted was not whether all the minor Y2K bugs got fixed, but whether critical services were delivered. The world's measured strategy of devoting significant resources to tackling critical infrastructure first and saving less critical problems for later worked splendidly.