The Pakistan Development Review
38 : 4 Part II (Winter 1999) pp. 1037–1056

Y2K Interruption: Can the Doomsday Scenario Be Averted?

NABEELA ARSHAD, DURR-E-NAYAB, and ARSHAD J. MINHAS

1. INTRODUCTION

The management philosophy until recent years has been to replace the workers with computers, which are available 24 hours a day, need no benefits, no insurance and never complain. But as the year 2000 approached, along with it came the fear of the millennium bug, generally known as Y2K, and the computers threatened to strike!!!!

Y2K, though an abbreviation of year 2000, generally refers to the computer glitches which are associated with the year 2000. Computer companies, in order to save memory and money, adopted a voluntary standard in the beginning of the computer era that all computers automatically convert any year designated by two numbers such as 99 into 1999 by adding the digits 19. This saved enormous amount of memory, and thus money, because large databases containing birth dates or other dates only needed to contain the last two digits such as 65 or 86. But it also created a built in flaw that could make the computers inoperable from January 2000. The problem is that most of these old computers are programmed to convert 00 (for the year 2000) into 1900 and not 2000. The trouble could therefore, arise when the systems had to deal with dates outside the 1900s. In 2000, for example a programme that calculates the age of a person born in 1965 will subtract 65 from 00 and get -65.

The problem is most acute in mainframe systems, but that does not mean PCs, UNIX and other computing environments are trouble free. Any computer system that relies on date calculations must be tested because the Y2K or the millennium bug arises because of a potential for "date discontinuity" which occurs when the time expressed by a system, or any of its components, does not move in consonance with real time. Though attention has been focused on the potential problems linked with change from 1999 to 2000, date discontinuity may occur at other times in and around this period. These dates are:

1. **Special use of certain values in part or all of a date filed, e.g.,**
   - 9 September 1999: 9-9-99 used as a file marker or special instruction by some systems.

Nabeela Arshad and Durr-e-Nayab are Systems Analyst and Research Anthropologist at the Pakistan Institute of Development Economics. Arshad J. Minhas is Manager, Computer Systems, The Population Council, Pakistan Office, respectively.

- 1 January 2001: 111 used as a special instruction in some systems.

2. **Failure to recognise 2000 as a leap year, e.g.,**
   - 29 February 2000: Some systems do not recognise 2000 as a leap year.
   - 1 March 2000: Systems may carry erroneous data because of an unexpected leap day.
   - 31 December 2000: Leap year problem may not appear until day 366 is not recognised.
   - 1 January 2001: The systems may carry erroneous data because of an unexpected day 366.

The present paper deals with the issue of Y2K in six sections. After an introduction to the "millennium bug" in Section 1, the issues related to risk assessment and potential problems linked to the Y2K would be addressed in Section 2. Section 3 deals with compliance definition and standards, and the status of some commonly used software in the light of these standards. Section 4 pertains to matters related to risk correction and contingency planning to counter the potential damages of Y2K. Section 5 discusses Pakistan's position in the race against the Y2K. Finally, Section 6 addresses the original question that can the doomsday scenario be averted????

2. RISK ASSESSMENT AND POTENTIAL PROBLEMS

Risk Assessment

The Y2K problem is significant and will affect virtually everyone as a direct or indirect user of computer systems. There are four types of damage associated with year 2000 problems [Feiler and Butler (1999)]. They are:

- **Direct Damage** consists of the problems with internal systems on which an organisation relies. These are the problems that are most frequently addressed in remedy efforts. Direct damage may consist of failures or of incorrect processing. Many reported cases have not involved failures. For example, a purchase order tracking system that reports purchase orders with two-digit years of 00 as having occurred before those with the year 99 does not fail but in mid-January 2000 one may be unable to determine what products are ordered that month.
- **Indirect Damage** refers to problems that business partners—customers, vendors, etc. may encounter. For example, an organisation that can correctly account for its employees' time regulators and advisors may be unable to pay them because of failures at its bank or at a payroll-processing company. Indirect damage to one organisation is often direct damage to another.
- **Ambient Damage** is the general disruption caused by year 2000 problems. For example, a bank's telephone switchboard that is swamped by customers

calling to find out if the bank's computers have failed is ambient damage. In a very broad sense, the entire year 2000 analysis and remedy effort is ambient damage: a disruption to the global economy brought about by potential failures (direct and indirect damage).

- **Causal Damage** is damage that is embedded in products that an organisation has distributed to others. This includes computer hardware and software that they have sold as well as products that may have given away (e.g., spreadsheet templates a financial might give to potential customers to help them create a retirement plan).

The potential of the Y2K problem is difficult to quantify. The challenge is wide reaching and it is much more than just an issue for mainframe computers or even PCs. Many other types of systems and equipment have embedded microprocessors that handle date data and could be affected by Y2K problems. Microprocessors embedded within components of transportation systems, manufacturing facilities, security systems, networks, telephone systems, or power grids, may be dependent on date related information. Two possible failure scenarios are examined below.

Complete System Breakdown is obvious and therefore easy to detect. In this event, contingency plans can be implemented and immediate action can be taken to address the breakdown. For example:

- An order entry application might not allow any orders to be entered after the year 2000 if the application treats 00 as an invalid number. In this situation, it would become immediately apparent that application was not functioning properly due to the fact that business would be stalled.
- An embedded system that controls an obvious physical function such as an air conditioner control unit could have a problem if there was date handling built into the maintenance systems. The malfunction of this device would be obvious due to the lack of cool air.

Partial Breakdown is a more difficult problem to recognise and can have more far reaching consequences than that of a complete system failure. If a system only partially fails, it may not be obvious to the user of that system. In the case of financial transactions, a calculation error may produce results that the user assumes are correct. For example:

- A business phone system may experience subtle problems in some subsets of its features. In most cases, a dial tone will still be available and the phone may seem to function normally. The problem may occur with the reports that detail the duration of each phone call. For an organisation that uses this information for billing and/or tracking, the problematic reports may not be immediately recognised and automated billing systems may generate faulty invoices.

Potential Year 2000 Problem Leading to the Doomsday Scenario

Computers and software have become indispensable parts of business, commerce, and government. Almost all major corporations now use computers and software as primary tools for accounting, finance, sales support, personnel records, and to a significant degree, manufacturing and distribution. Banks and service organisations use computers and software for virtually all financial transactions. Government agencies use computers for all vital records and keeping track of data on almost every citizen. The Y2K problem would have been invisible if it had occurred in 1950 and only a minor annoyance if it had occurred in 1975 since computers and software were not yet key business tools. But when the problem occurs in 2000 it has at least the potential to damage the economies of every industry and every industrialised nation. The following is a list of some of the major kinds of problems that the Y2K glitch can cause unless software applications are corrected before the millennial date rollover.

- The Y2K may affect international air traffic control. Also of concern are potential date problems with airline reservation systems, aircraft maintenance systems, and on-board navigation and flight control software. A significant number of commercial aircraft may be grounded for an indefinite period, the insurance coverage is yet another troublesome prospect.
- Banking systems are also a major concern, the range of problems associated with this sector include automated teller machines operations, interest rate errors, electronic funds transfer errors, and the validity of all records associated with accounts. Bankruptcy is among the most troubling potential problems associated with the Y2K bug if it disrupts the electric power, shipping, telephones, etc. for a long enough period so that cash flow is severely blocked.
- Credit card processing is highly date dependent, and the credit card problems have already started to occur.
- Databases, data warehouses, and data mining are subject to very severe calendar date problems. Y2K may put an abrupt end to online analytical processing and other database activities, which is among a serious manifestation. Companies and governments have become so dependent upon online databases that there are no effective contingency plans in place should the Y2K cause major database disruption.
- Defence software is very susceptible to the Y2K problem and thus very important to national security. Some of the defence implications of Y2K problem include the need to update critical applications on board submarines and ships at sea, satellites in space, the guidance and control systems of torpedoes, ballistic missiles and other sophisticated weapon systems.

- Electric power generation and distribution systems are of serious concern, since voltage spikes and frequency changes may occur as well as total disruption of service, thus this failure mode can be hazardous. Also gasoline production, distribution, and availability is a topic of some concern as every step in gasoline production from extraction of crude oil through refining through distribution is highly automated.
- Government responses to Y2K problem range from fairly competent to shockingly incompetent. Major concerns include errors in tax bills, registrations of automobiles and births and deaths, and other government records.
- Health care systems are often error-prone and therefore there are concerns associated with its every aspect including distribution of pharmaceutical productions, failures of complex medical instruments, and errors in billing and financial applications.
- Income tax errors are expected to be the most serious manifestation of the Y2K event. The worst case scenario for taxation is that the problem will be so severe that the present graduated income tax structure may not survive the event.
- Infrastructure is the complex of facilities and services that allow a country to operate normally: i.e. roads, transportation systems, communication systems, public utilities etc. Y2K problem has the potential to damage the infrastructure for periods that may run from a few days to many weeks.
- Insurance applications are a major source of concern. The insurance industry is itself worried about the possible damage claims that might be filed. The fact that when risk and casualty insurance companies become aware of massive claims, they may balk at making payments and hence leave clients in severe financial distress is of great concern along with severe and enormous litigation potentials of Y2K law suits.
- Mail and shipping services disruptions is one of the more hazardous potential problems associated with the Y2K issue as all of these depend upon aircraft and fleets of vehicles, and some also utilise computerised tracking systems.
- Manufacturing applications using automated tools and computer-controlled assembly lines are very susceptible to the year 2000 date problem. Unfortunately, the software is embedded in many kinds of tools and machines and repairs require replacement of chips rather than simply seeking out dates and fixing them. The concern is that a number of manufacturing assembly lines will stop working for an indefinite period. Supplemental concerns include inventory management and delivery schedules of “just in time” components whose schedules may be thrown off.
- Nuclear safety is another topic of concern. Nuclear plants do not always

have very impressive safety records and the chaos associated with the year 2000 problem may make things much worse. Of particular concern are nuclear plants in Russia and Eastern Europe where the Chernobyl incident has long highlighted the fact that safety is poorly managed. However, the U.S. nuclear industry also needs attention.

- Pay cheques and payroll applications are at severe risk. A very significant percentage of pay cheques in January 2000 AD will probably be incorrectly calculated. The exact number is unknown, but perhaps 15 percent of cheques produced by software payroll packages may be incorrect unless Y2K compliance is accelerated in this critical domain.
- Personal computers and many commercial software applications have Y2K date problems. Some of these problems may do no harm, but date errors in financial packages, spreadsheets, or payroll packages may be quite serious. Lawsuits against personal computer manufacturers are likely too, assuming if their internal clocks fail various year 2000 compliance tests.
- Personnel systems and personnel databases are filled with date information, and some of the dates are indirect and calculated dynamically, which makes them hard to find and correct. Errors in personnel records can affect eligibility for pensions, pay raises based on seniority, stock vesting schedules, and a number of other personnel events.
- Process control applications are often date sensitive. This means that a number of key industries may experience shutdowns or malfunctions, with the most troubling of these being oil refining, steel manufacturing, and chemical production.
- Railroad transportation is highly automated and controlled by computers. Some of the potential problems would include losing track of freight cars, and possible safety hazards if rail-scheduling systems are disrupted.
- Recession or depression is one of the most troubling possibilities of the Y2K problem. If a significant number of businesses and government agencies fail to achieve Y2K compliance, then the damage and recovery costs may push a significant number of organisations into bankruptcy, which in turn would sharply elevate unemployment rates. The primary debate among economists who study the year 2000 problem is not whether a recession may occur, but rather its severity and duration.
- Security systems are often date sensitive. One of the more annoying kinds of Y2K problem may be failure of both building security and computer security applications, which can prevent people from entering their office buildings in the former case, or using their computers in the latter case.
- Stock market applications, and also bond market applications, are likely to have double problems caused by the need to make Euro-currency repairs and year 2000 repairs on parallel schedules. The points of concern are

possible shut downs or incorrect recording of stock and bond transactions.

- Stock values are likely to be unpredictable under the impact of Y2K problem. Companies that achieve Y2K compliance may see an increase in value, but companies that are not compliant, and are sued as a result may witness a severe decline in stock value. The stock situation is uncertain but the overall prognosis is that the year 2000 event may trigger a sharp decline in stocks and bonds when the seriousness of the year 2000 problem is realised at the turn of the century.
- Tax increases due to the high costs of year 2000 repairs are not unlikely. The cumulative costs of fixing government software will be high, and the money is often unplanned and unbudgeted. Either tax increases or service reductions, or both, are the possible after-shocks of the year 2000 problem. Tax revenue reductions are also a topic of concern. Since the costs of year 2000 repairs are quite high, many public and private companies will report losses or earnings reductions for 1998 through about 2002. This means that projected tax revenues may be lower than planned at every governmental level for as long as five years. For example the State of New Jersey had projected tax revenue declines of several hundred million dollars due to the year 2000 problem.
- Telephone switching systems are highly automated, and the automation is extremely sensitive to date and time information. Of concern is the fact that telephone-switching systems may shut down as a result of the Y2K problem. There are also concerns about possible billing errors, but the main topic is whether the switching applications themselves will achieve Y2K compliance. Adding to the uncertainty of the Y2K problem in telecommunication context, many switching systems are written in languages such as C, CHILL, and CORAL, which lack effective Y2K support tools and also may have shortages of trained programmers.
- Testing the year 2000 repairs is perhaps the most complex form of testing ever associated with software applications. The reason for this is because the date-sensitive information used by many applications comes in from external sources, such as clients, suppliers, or government agencies. This means that some forms of Y2K testing must go outside the enterprise, and include joint testing among all data providers and data users. In many industries such as banking and telecommunications, effective Y2K testing may even require co-operative testing among direct competitors. The implications of poor testing of year 2000 updates are very serious, and can lead to software failures and even to possible litigation.
- Trucking systems in the industrialised nations are highly automated and also depend upon the ability to pump diesel fuel at thousands of locations adjacent to all major highway nets. If the Y2K problem causes widespread disruption of electric power for more than a few days, then the ability to

move goods by truck will be reduced significantly.

The paper does not imply that the problems will occur, but there is no doubt that the problems might occur unless year 2000 repairs are diligent and effective. The Y2K problem is unique in that it affects many critical computerised applications simultaneously, and there are no effective ways to avoid the problem except methods that involve both costs and effort.

3. COMPLIANCE DEFINITION AND STATUS OF SOFTWARE

Compliance Definition

For any system to be Y2K compliant it should fulfil the following definitional rules [Roberg (1999)]:

Rule 1: General Integrity

No value for current date will cause any interruptions in operation, as the data on the operating system advances into the 21st century without causing any problems in the software.

Rule 2: Data Integrity

Data based functionality must behave consistently for dates prior to, during and after year 2000. The software should be able to process dates internally and represent them correctly.

Rule 3: Explicit/Implicit Century

In all interfaces and data storages, the century in any date must be specified either explicitly or by unambiguous or inferencing rules, i.e., either the software uses four digit year values or a century indicator or a two digit year value that cannot be misinterpreted.

Rule 4: 2000 as a Leap Year

Year 2000 must be recognised as a leap year.

There are different levels of compliance to asses the status of existing machine, software, embedded system, etc., These standards are used to model the strategy designed to make the systems compliant. They are:

Level1 : Software should be compliant in the sense that no dates past, present or future would cause a failure in processing, or dates would not be used for purposes that are not related to the calendar. Otherwise, there should be no date data in the technology whatsoever.

Level 2 : Technology satisfies the provisions of DISC PD2000-1[1].

[1]DISC PD2000-1 is a definition of Year 2000 Conformity Requirements by Delivering Information Solutions to Customers through International Standards. DISC has specific responsibility for the management of Information Systems and Communication Technology Standards.

Level 3 : Technology satisfies the provision of IEEE P2000-1[2].
Level 4 : Technology would operate correctly until or after 2000-01-01.
Level 5 : Technology would not fail materially after 2000-01-01.
Level 6 : Technology would fail, though not materially, before 2000-01-01.
Level 7 : Technology would fail materially after 2000-01-01.
Level 8 : Technology would fail materially before 2000-01-01.

Status of Commonly Used Software

Based on the rules given above the status of some of the most commonly used software can be divided into three categories, namely:

- Not compliant.
- Essentially compliant with minor problems.
- Fully compliant.

The status of some of the software according to these categories is given in Table 1

Table 1

Compliance Status of Commonly Used Software

Not Compliant	Compliant with Minor Problems	Fully Compliant
	Operating Systems	
• Novell Netware 3.11	• MS-DOS 6.0, 6.2 • Windows 3.11 • Windows NT server SP3 • Novell Netware 3.12	• Windows 95, 98
	Database Software	
• Paradox 3.5, 4.5, 5.0 • SybaseIQ 11	• Informix 4GL for window • Paradox 7.0 • MS Access 2.0 • Microsoft Access 95 v7.0 • Microsoft Access 97 v8.0	• Paradox 8.0 • Clarion v2.11, v4.0
	Spreadsheet Software	
• Corel Quattro Pro v1, v4 • Microsoft Excel v4.0	• Corel Quattro Pro 6 for Win 95/NT • Corel Quattro Pro 6 for Win 3.X • Lotus123 v5.01 for Win95 • Microsoft Excel v 5.0 • Microsoft Excel 97 v 8.0	• Quattro Pro for Win 5.0 • Corel Quattro Pro for windows v 8.0 • Lotus 123, v4.0 for DOS • Lotus 123 v4.0 for Win 3.1
	Word Processing Software	
• Word Perfect 5.1	• Corel Word Perfect for Win 6.0 and 5.2	• Microsoft Word v6.XX • Microsoft Word 97 v8.0 • Corel Word Perfect 5.1
	Statistical Software (as of latest versions)	
	• SHAZAM • LIMDEP	• SPSS • STATA • SAS
	Internet Software	
• Internet Explorer v3.0X • Netscape Navigator		• Internet Explorer v4 and above • Front Page Explorer 3.0.2.926 • Netscape Communicator

Source: www.sdnp.org.

[2]IEEE P2000-1, is a definition for "Year 2000 Compliance" by the Institute of Electrical and Electronics Engineers (IEEE) Computer Society Year 2000 Standards Projects.

4. RISK CORRECTION AND CONTINGENCY PLANNING

Management can prepare itself by looking at how key industries are likely to be impacted under various year 2000 scenarios that may arise during the transition window. The transition window is the period of time where year 2000 problems escalate, peak and taper off. We have, as of late 1997, already entered this transition window, due to the fact that Y2K related problems have started occurring.

The problems are expected to ramp up, peak, and ram down over a period of many years. The activities that management must plan for and deal with during these time frames can essentially be divided into project management, crisis management and cleanup management.

- **Project Management** means taking care of the planning and conversion work required fending off year 2000 problems. The year 2000 project life cycle as shown in Figure 1 starts right from realisation of the problem and ends when all tests and certifications have been dealt with.
- **Crises Management** begins right around New Years Eve 1999 and runs until an organisation once again achieves stability in all of its operations.
- **Cleanup Management** during the post 2000 period can include options like outsourcing the IT environment, utilising system redevelopment strategies, choosing to utilise off-the-shelf application packages, etc.

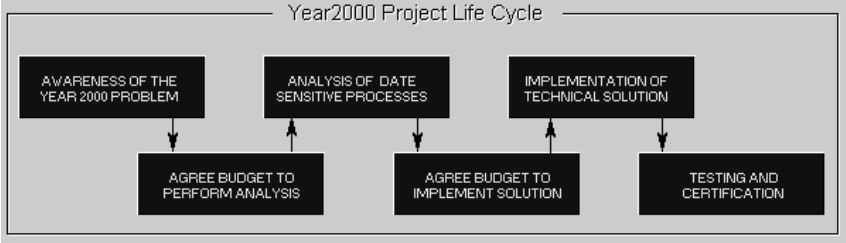

Fig. 1. Year 2000 Project Life Cycle for Risk Management.

Citing the potential economic impacts of the year 2000 problem is aimed at alerting executives and government leaders to the overall and cross-industry problems so they can be prepared to address them during the year 2000 transition window.

The year 2000 risk correction management must be able to support all three phases of the problem including the project management, the crisis management and the cleanup management. One of the critical tasks is establishment of a crisis management team that can work through problems and make quick decisions, when failure arises. This team can be best comprised of a small group of IT and business professionals, who can make decisions without the need for lengthy meetings or group consensus.The required speciality risk correction management functions can be shown with the help of Table 2.

Table 2

Key Players and their Specialised Tasks in Risk Management

	Key Players	Task
1	Business Unit Co-ordinators	• Work with application units to prioritise short-term corrections.
2	Application Unit Co-ordinators	• Ensure application area resources availability. • Provide input to contingency plan invocation.
3	Hot-line Interface Co-ordinators	• Provide second-level support to hot line questions, and serve as liaison to business unit and application unit.
4	Mainframe Systems Software and Hardware Co-ordinators	• Interface with vendor and operations for problems. • Work with application and business unit to ensure that system repairs are prioritised by business critically.
5	Network, Distribution Systems Software, Hardware Co-ordinators.	• Interface with vendors and operations for any problem in network environment. • Work with application and business unit co-ordinators to ensure that network repairs are prioritised by business critically.
6	Supplier Compliance Managers	• Function as first point of contact for all reported supplier problems. • Work with business unit co-ordinators to ensure that supplier-related decisions (triage, replace, need) are prioritised by business criticality.
7	Interface Compliance Managers	• Manage SWAT team support functions to review errant data detected by application or business units. • Work with application and business units to ensure that interface-related problems are corrected based on business criticality.
8	Embedded Technology Compliance Managers.	• Co-ordinate any problems that may arise with security, elevator or other computerised facility functions. • Work with vendors to get problems fixed immediately.
9	Communication Managers	• Function as first point of contact for external queries regarding Y2K problem. • Manage damage control process • Work with project office, communication department and senior executives to craft stockholders, customer and media statements.
10	Third Party Support Co-ordinators	• Handle all consultant/contractor co-ordination for project. • Ensure that additional staff is available as needed to fix application or other aspects.
11	Project Office Director	• Co-ordinates all activities of crisis management team. • Track triage, contingency and other priority-based decisions in central database. • Provide situation analysis to senior management legal counsel and internal auditors on a regular basis. • Assign additional staff as required to manage crises smoothly.

Transition management, particularly during the critical crisis management time frame will require rapid situation analysis and fast decision by small teams. Major decisions, including invocation of triage and higher-impact contingency options, may require one or more units of an organisation to make a quick consensus decision. When these situations arise, senior executives must get involved quickly to make a call.

Formulation of the Y2K compliance strategy is a two stage process as shown in Figure 2. Stage 1 is concerned with issues like system inventory, critical system tests and preparation of TORs as an agreement to proceed to the analysis stage. Stage 2 deals with assessment of internal impacts, time to failure and exploration of possible option to combat the potential problems.

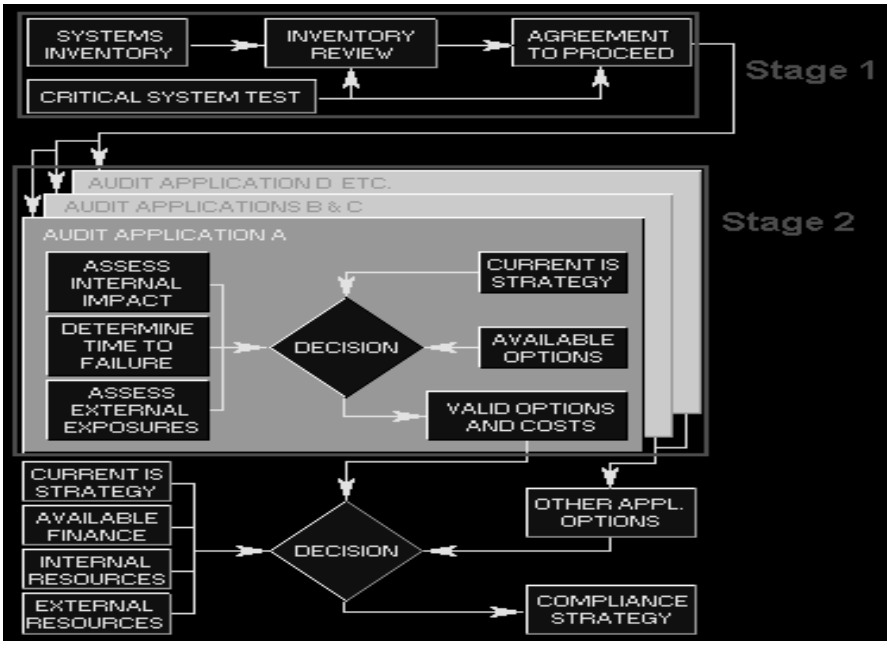

Fig. 2. Stages in Planning and Conversion.

The operating environment of an organisation dictates which issues will arise and how they are to be resolved. Organisations should utilise risk management and contingency planning as input to the crises management planning process. Many problems are expected to arise due to the internal failures or unanticipated situations that occur within the domain of IT or in various other units of an organisation. Planning team therefore must consider the following major internal considerations:

- End-user calls, about problems with the IT supported application.
- System software and hardware failures.
- Network failures.
- Embedded system problems in facility system.

Along with internal preparation it is important to be prepared to manage problems related to critical dependencies. The following is a non-exhaustive list of important consideration:

- Customer calls impacted by application system failures.
- Government regulators call after discovering an irregularity.
- Delays in government provided services.
- Critical infrastructure failures as:
  - Electric Power.
  - Gas.
  - Telecommunication.
  - Internet/E-mail System.
  - Water and Sanitation.
- Problems related to service supplies as:
  - Banking/financial services.
  - Transportation.
  - External IT process services.
  - Shipment delays.
  - Health care.

Contingency Planning and Triage

It is important to form a group called contingency planning and triage group to act as a nerve for monitoring and triggering contingency and triage strategies. This group can be comprised of high-level executives, key IT executives, the embedded systems co-ordinator facility co-ordinator, supplier co-ordinator, legal counsel and other team representatives as required.

The contingency plan triggering criteria can include following major considerations.

- Defining who has the authority to pull the trigger on a contingency plan.
- Establishing planned and unplanned triage criteria.
- Who tells what to whom.
- When and how to notify a party when bad data has been sent to them.

5. PAKISTAN'S STATUS ON THE Y2K

With the Year 2000 less than two months away is Pakistan Y2K ready? The answer to this question varies from no to yes, maybe and hardly, depending on who is expressing his/her opinion. Pakistan that has 138 mainframes and 1649 mini-computers in the government and private sector [Pakistan Computer Bureau (1999)] emerged quite late in getting concerned about Y2K. It was only in November 1998 that a national task force was set-up to create awareness and co-ordinate Y2K compliance activity. According to the Pakistan Computer Bureau (PCB) the major area of concern is the power (mainly WAPDA), and communication (mainly CAA and PTCL) sectors. WAPDA has identified quite a few generating stations where there is a possibility of such problems. Likewise Civil Aviation Authority (CAA)

needs some urgent effort on this account as its flight information and radars need compliance. On the whole the "National Task Force on Y2K" has sent directives to all major government and private organisations including those in the transport, medical, manufacturing, communication, banking and finance sectors, on the following issues:

- General understanding of the importance of contingency planning for year 2000.
- Having a year 2000 action plan, with sufficient resources allocated towards fixing and testing the highest priority deliverables.
- Developing a prioritised list of core business functions and essential services.
- Analysis of risks and potential impact of a year 2000 failure to core business functions and essential services.
- Preparation of a simple and easy to understand plan of action to deal with potential year 2000 failures to ensure business and service continuity.
- Developing appropriate trigger mechanisms for activating contingency plans.
- Testing the contingency plan by simulating potential year 2000 disruptions.
- Updating and testing emergency management and disaster recovery plans.
- Having an emergency management team in place for January 1, 2000 with assigned responsibilities.
- Communicating the contingency and emergency management plans with the organisation and with customers, suppliers and stakeholders [PCB (1999)].

As the information collected by the PCB shows, large organisations in Pakistan are not yet fully dependent on technology, which in the present circumstances is blessing in disguise of sorts. Among the major organisations in Pakistan surveyed by the PCB, as Table 3 shows, hardly 30 percent are fully dependent on technology.

Different organisations have adopted different options to remedy the situation and make their work systems Y2K complaint. As Table 4 shows, all three options of repairing, replacing and retiring are being used by the surveyed organisations. Since certain organisations had equipment that were so old that repairing them was not possible, there was no option but to retire this equipment, and replace it with new Y2K compliant one.

Coming back to the main question, What is the Y2K compliance status of organisations in Pakistan? The results given by recent follow up survey conducted by the PCB shows that 40 percent of the major organisations are already Y2K compliant,

Table 3

Technology Dependency in Various Large Organisations in Pakistan

Organisation	Not Dependent	Partial Dependent	Moderately Dependent	Fully Dependent
Habib Bank Ltd.	–	–	Yes	–
United Bank Ltd.	–	–	Yes	–
Pakistan Audit Deptt.	–	Yes	–	–
ADBP	–	–	Yes	–
State Bank of Pakistan	–	–	Yes	–
KESC	–	–	Yes	–
State Life Insurance	–	–	Yes	–
PTCL	–	–	–	Yes
Sui Southern Gas Corp.	–	–	–	Yes
WAPDA	–	Yes	–	–
PIA	–	–	–	Yes
Civil Aviation Authority	–	–	Yes	–
National Tele. Corp.	–	–	–	Yes
Pakistan Railways	–	–	–	Yes
Karachi Port Trust	–	Yes	–	–

Source: PCB (1999).

Table 4

Options for Remedy Adopted by Different Organisations in Pakistan

Organisation	Repair	Replace	Retire
Habib Bank Ltd.	Yes	Yes	Yes
United Bank Ltd.	–	–	–
Pakistan Audit Deptt.	Yes	Yes	Yes
ADBP	Yes	Yes	Yes
State Bank of Pakistan	Yes	–	–
KESC	Yes	Yes	–
State Life Insurance	–	Yes	–
PTCL	Yes	Yes	Yes
Sui Southern Gas Corp.	Yes	Yes	Yes
WAPDA	Yes	Yes	–
PIA	Yes	Yes	–
Civil Aviation Authority	Yes	Yes	Yes
National Tele. Corp.	Yes	Yes	–
Pakistan Railways	–	Yes	–
Karachi Port Trust	–	Yes	–

Source: PCB (1999).

while the remaining have a deadline of November, 1999 at the maximum. As Table 5 shows among the vital organisations still to reach the compliant status are PTCL, WAPDA, PIA and CAA. These organisations however, state to be facing no problems in their effort to be Y2K compliant, and are positive to be ready by the crunch time, i.e. turn of the century. However, as a precautionary measure PIA, like many other international airlines, has decided to halt their flight operations to and

from Pakistan for 18 hours starting on the evening of December 31, 1999. Notwithstanding any unforeseen occurrence, on the whole the picture in Pakistan does not appear to be all that bleak.

Table 5

Y2K Compliance Status of Large Organisations in Pakistan

Organisations	Y2k Status
Habib Bank Limited	Compliant
United Bank Limited	Compliant
State Bank of Pakistan	Compliant
Pakistan Steel Mills	Compliant
Port Qasim Authority	Compliant
Karachi Port Trust	Compliant
National Bank of Pakistan	Compliant
Pakistan Railways	Compliant
Karachi Electricity Supply Corporation	Compliant by September '99
Pakistan Telecommunication Corporation Limited	Compliant by September '99
Sui Southern Gas Corp.	Compliant by September '99
Sui Northern Gas of Pakistan	Compliant by September '99
Pakistan International Airlines	Compliant by September '99
Oil and Gas Development Corporation	Compliant by September '99
State Life Insurance	Compliant by October '99
Pakistan Audit Department	Compliant by October '99
Water and Power Development Authority	Compliant by November '99
Civil Aviation Authority	Compliant by November '99
Pakistan Ordinance Factory	Compliant by November '99

Source: PCB (1999).

6. CAN THE DOOMSDAY SCENARIO BE AVERTED?

In the end we come back to our original question: Can the doomsday scenario be averted? Given proper measures are taken, as discussed earlier in the paper, the answer to this question is "YES"!!!

There are six main layers of exposures to the Y2K problem [MTN (1999)]:

- Hardware.
- Operating system.
- Application and runtime libraries.
- Documents and spreadsheets.
- Custom code.
- Data interfaces.

The most common hardware problem suspected by the Y2K is related to the computer's Real Time Clock (RTC) and Basic Input/Output System combination (BIOS). It is essential to identify the BIOS make and version, and to test it forY2K

compliance in order to avoid any problem. If the century rollover code is missing from the BIOS, the RTC century value would not be updated. Newer operating systems like Windows NT 3.51 (with service Pack 5 plus Y2K fixes), Windows NT 4.0 (with service pack 4 plus Y2K fixes), Windows 98 (with Y2K fixes) and Windows 2000 would recognise 1900 as an error case and will rollover to the next century by setting the date to 2000. Thus, if the BIOS reverts to 1900 every time the system reboots, these Y2K fixes in the operating systems will put forward the RTC to 2000 averting any problem.

Similarly, updates or repairs, through patches, are now available for most of the software under use to make it Y2K compliant. As Table 1 showed some of the old software is totally not compliant. Nothing much could be done about it to make it Y2K compliant, however solutions exist for those that have minor problems. In many cases easy downloads are available which can make them Y2K compliant. For example, old software like LOTUS 1-2-3 version 5 for Windows 3.1 can be made compliant by downloading a patch from the site:

http://www.support.lotus.Compliant/homeframe/nsf/pages/123w

Or like for Microsoft Access 95 from the site:

http://officeupdate.microsoft.compliant/articles/095Y2K/factsheet.htm

In some cases however, there would be a need to upgrade the programmes as patches alone would not be sufficient.

The doomsday scenario can be very well averted if any organisation or person takes timely decision and action on whether to fix, replace or retire the existing systems or applications which are not Y2K compliant. Any such decision should be made after a Y2K evaluation based on complete inventory and analysis of existing information technology base. The decision to fix, replace or retire systems or applications should be made after considering the following things [MTN (1999)]:

- Fix the code if you have access to and an understanding of the source code.
- Re-host on same platform. More often than not this implies custom development work on that platform. This is a viable option to maintain knowledge base and expertise.
- Re-host on a new platform. This is commonly known as the “replacement” strategy.
- Outsource a broken business function, alleviating the pressure on internal human and physical resources.
- If time and human resources run short, retire systems that are deemed critical while re-mediating others to remain functionally problem-free.

If all these factors are given due consideration it could be said that the doomsday scenario presented regarding the Y2K would be safely averted. Even if

some of the fears prove to be true, it still would not be as bad as doomsday, as very rightly put by Lagesse (1999):

> "There will be casualties. But we will endure (no doubt in various stages of undress) and learn and eventually time will heal the wounds of those that have survived. To believe anything else is to ignore the history of human ingenuity in crisis situations. History also suggests humans are better at cleaning up than preparing. Y2K is no different except that this time everyone has a long lead-time to prepare- operationally and financially".

REFERENCES

Lagesse, Doug (1999) How to Financially Protect your Business from Y2K Business Interruption- The essential workbook. www.y2krg.com.

MTN (Microsoft TechNet) (1999) www.microsoft.com/technet/year2k.

Pakistan Computer Bureau (PCB) (1999) www.pcb.gov.pk.

Feiler, Jesse, and Barbara Butler (1999) *Risk Assessment: Four Types of Damages*, Proceedings on conference on Y2K, www.itpolicy.gsa.gov/mks/yr2000/y2kconf/.

Roberg, Elmar (1999) *Y2K Compliance Issues*, Proceedings on conference on Y2K www.itpolicy.gsa.gov/mks/yr2000/y2kconf/.

The Y2K "Managing the Challenge" Self Help Tools Video, U.S. Department of Commerce, www.doc.gov/y2k/.

Chandrasekaran, Rajiv (1998) Year 2000 Preview. *Washington Post*, Jan. 2.

Ridder, Knight (1999) Millennium Bug May Already Be At Work in Financial Institutions. *Lubbock Avalanche*, December 4, 1997.

Sunday Times (1997) Millennium Bug Alarms Unilever. December 21.

Newsday (1998) Year 2000 Glitch Hits Credit Card/Automated Approval Stymied. January 3.

Adams, Christopher (1997) Insurance: US Insurers Limit Their Losses. *Financial Times.* December 22.

Guzman, Eneida (1997) Apocalypse 2000. Investor.mns.com, November 13.

Zells, Lois (1997) The Project Office Answer. *AD Trends.* April.

Gould, Jay (1997) Myths of the Millennium. *USA Weekend.* September 19-21.

www.sdnp.org

www.usatoday.com/life/cyber/tech/

www.cnet.com/y2k/

www.netscape/technews/

www.bsi.org.uk/disc/

www.computer.org/standards/

Comments

The Year 2000 Problem or the Millennium Bug, was caused by standard industry practice to use two-digits for the year in electronic devices. Although fundamentally a technical problem, it poses a major threat to business continuity thus making it a business problem. The repercussions of the problem were not confined to information technology alone. Almost any area that uses the microchip was considered vulnerable. The millennium bug could affect computers and microprocessor-based systems, microprocessor-embedded systems and installed software in hospitals, financial institutions, air traffic control, power generation, gas distribution, telecommunication systems, and transport. The Government sector, being the largest public sector "enterprise" in any country, was likely to be most affected. The top priority areas cover Power Generation, Telecommunication, Health, Finance and Transport.

Risks Faced

A number of constraints that pose risks to the successful implementation, needed to be taken into consideration in any Y2K programme initiative, whether in public or private sector including the following:

- Short time span left before the advent of Year 2000.
- Prevalence of inertia on the part of policy-makers.
- General paucity of resources (including budgetary allocations).
- Legacy systems written in pre-fourth generation languages, with no documentation.
- Diverse embedded systems that pose most difficult situations.

Contingency Planning

To counter the possibility that critical systems may not operate effectively and the probable failure of less critical systems, all organisations need to create contingency plans. At the operational level this becomes a crucial issue that needs to be addressed. The problem with the millennium bug is that possibilities exist for concurrent or multiple coincident failures. Contingency plans in the Year 2000 context need to be drawn up with great care as to assumptions made about availability of services not directly affected. Contingency Planning is therefore, perhaps, one single area that calls for concerted co-operative initiative by organisations and businesses.

Measures Undertaken

Before the clock ticks the arrival of Ist January, 2000, all mission critical systems must be Y2K ready. The Pakistan Computer Bureau as the focal point of Y2K activities has been playing its pivotal role in creating awareness and monitoring

the status of Y2K Readiness in important sectors and organisations. The National Task Force on Y2K in Pakistan headed by Director General, Pakistan Computer Bureau included the representatives of Ministries of Finance, Water & Power, Communication, Petroleum and Natural Resources, Railways, Defence Production, Aviation, Health and all major stake holders in government as well as private sector.

A number of important decisions relating to the issue were taken and implemented. The measures taken by the Task Force to create awareness and monitor the status of the pace of work on Y2K include:

(i) Seminars and Workshops in Islamabad and provincial headquarters for the managers and professionals government as well as private sector.
(ii) Identify critical state organisations in important sectors like Power Generation, Telecommunications, Shipping and Air Transport, Banking etc.
(iii) Assessment Surveys on Y2K Preparedness at major state organisations undertaken asking them to report their status of Y2K related activities.
(iv) Guidelines for Y2K Preparedness and Contingency Planning prepared and issued for immediate adoption and implementation by organisations and businesses.
(v) Study teams comprising professionals constituted to visit important organisations to find out their preparedness status and render all possible assistance.
(vi) The target date of 30th September, 1999 was fixed for internal compliance of mission critical systems in individual organisations.
(vii) The heads of major state organisations made responsible for Y2K compliance in their organisations.
(viii) Y2K Control Room established in the Bureau and information about Y2K activities and status in Pakistan placed in the Web Site.
(ix) Publicity through print media in major English and Urdu language newspapers all over the country.
(x) Appointed consultants to study and report the Y2K status in Power, Energy, Communication, and Transport sectors.
(xi) Status reports by major organisations and sectors for public confidence building at National Seminar held at Islamabad.
(xii) Audit teams for testing and verification of systems that have already been reported Y2K compliant.
(xiii) Y2K Seminars for Health Sector held at Karachi and Islamabad attended by health officials, hospital administrations and medical practitioners.
(xiv) Y2K Control Centres for Millennium Roll Over on 31st December.

Ijaz H. Khawaja

Pakistan Computer Bureau,
Islamabad.