COMPUTER SYSTEMS AND THE MILLENNIUM

- *How are computer systems affected?*
- *What are the implications?*

POST note 89 December 1996

Many computer systems may fail in transition to the Year 2000, because of the way they store and manipulate dates. There is concern over the possible consequences, and Government initiatives are underway to raise awareness. Parliamentary interest in this has included a Commons debate in June 1996 and a possible private Members Bill.

This note analyses the potential scale of the 'date change problem' and the policy issues raised.

WHAT IS THE DATE CHANGE PROBLEM?

In the past programmers were under pressure to save as much space as possible and generally abbreviated the date by using two digits for the year - 76 for 1976 etc. In such systems, the Year 2000 will become 00 and it has been apparent for some time that this may cause problems - for example the computer will calculate the interval between 1976 and 2001 as 01-76= **minus** 75 years. It is easy to imagine the problems this causes if checking someone's age, how long goods have been in store and other routine tasks; other problems arise in:

- **interpretation** (e.g. does '00' mean 1900, 2000, etc.);
- **validation** (systems may not accept '00' as valid);
- '**day of week**' calculations (e.g. January 1, 2000 will be a Saturday, whereas systems using '00' dates may give 'Monday', the first day of 1900).
- 2000 is a **leap year, but** some programmers did not realise this[1]. Their programs will not recognise February 29, 2000 and calculate days incorrectly.

These and other date-related errors may have difficult-to-predict and far-ranging effects, ranging from generating an incorrect date, financial calculation, etc., to causing a whole computer system to 'crash'.

WHAT WILL BE AFFECTED?

All computers are potentially affected - this includes the **'mainframe**' computers which typically provide core 'headquarters' functions such as maintaining customer databases, payroll and stock control for large businesses, financial institutions, Government Departments, etc. Equally vulnerable are the **minicomputers** which typically run applications for medium-sized business, often interacting and sharing data with other computers through **computer networks**. **Personal computers (PCs)** used for 'desktop' applications such as word processing, spreadsheets, etc. and in networks are also at risk. Even recent machines and software often contain a '**legacy'** of old programs or hardware which were prepared when two digit years were standard, and systems which have already encountered date-related problems because they look forward several years (e.g. for mortgage calculations) may have been 'fixed' using 'patches', rather than changing date formats throughout all systems, and still be vulnerable.

The two digit date can appear in many different parts of systems. Based on early experiences of analysing date change problems, **about 80% of all mainframe computer systems contain two digit year references** in their programs (software). PCs have built-in programs ('operating systems' such as 'DOS' and 'BIOS') which, in many cases, do not handle the century transition correctly. Moreover, date references occur in many different parts of PC software. Thus, the ubiquitous Microsoft (MS) Windows 3.1 operating system appears to handle the century transition correctly in its calendar, but its File Manager does not. Unpredictable problems may arise in applications - for instance, older versions of MS Word will not allow work to be saved after 1 Jan, 2000!

Computer 'chips' are also at the heart of a wide range of **electronic and mechanical devices**, from cash registers, to televisions and video recorders, security doors (e.g bank vaults, 'swipe card' entry systems), cars, aircraft, process controllers, etc. These **'embedded systems**' constitute a large but difficult to quantify class, both in terms of vulnerability to date change problems and their effects.

Some forecasters see a danger of failures in:

- **payroll systems**, so that workers cannot be paid;
- **financial records**, losing track of investments;
- **invoicing systems** - e.g. failure to generate bills, charging 100 years of interest;
- **telecommunications networks**;
- **government systems** - e.g. benefit payments, criminal records, medical records, revenue collection;
- **utilities** (elecricity and gas suppply, etc.);
- **safety critical systems** such as air traffic control, defence equipment, etc.;
- **unpredictable behaviour of embedded systems**, whether elevators, cars or medical equipment.

Because of **the ubiquitous** nature of the effects and the **very short time interval** in which they may act at the turn of the century, some see a danger that a 'domino effect' might cause IT systems to fail throughout whole sectors of the economy. So far however, documented examples have been on a more limited scale (**Table 1**).

1. Years ending in '00' are not leap years unless they are divisible by 400.

Table 1 SOME EXAMPLES OF DATE CHANGE PROBLEMS

- **In 1992, Mary Bendar of Winona MN, USA was invited to join kindergarten class because she was born in '88 (she was 104 years old);**
- **At least one US state has changed its driving licence renewal from 4 to 3 years because of problems of having an expiry date after 2000;**
- **Problems authorising credit cards with '00' expiry dates;**
- **A supermarket (Marks & Spencer) computer ordered new canned goods to be discarded because sell-by dates were post-2000;**
- **A multi-M£ UK hospital body scanner which would not work on 29 Feb 1996 because it couldn't handle leap years.**

WHAT ARE THE SOLUTIONS?

Solving the century date change problem appears almost trivial: find all two digit year references, 'fix' them and test the system still works. However, none of these stages is straightforward. For instance, IT systems used by governments and large organisations are **very large** (e.g. the Department of Social Security has more than 200 mainframe computers.) Typically, each system has more than 100 million lines of code in thousands of different programs, all of which must be checked and corrected. Databases pose similar challenges with dates common in the many millions of records. Additionally, the large numbers of individual and networked PCs throughout most organisations present separate challenges outside the immediate control of central IT units.

Amending the software is complicated by the fact that around 2400 different programming languages have been used since the 1950s. Many of these are no longer 'supported' by a manufacturer, and documentation may be hard to come by; or changes made over the years may mean that current programs bear little resemblance to the original. Furthermore, the ways that dates appear in and interact with programs can be far from straightforward, and vary between programmers.

The 'obvious' measure of **expanding all two digit year references** to four digits is a complete and 'permanent' solution, but requires both programs and data records to be altered, and both will grow in size significantly. Alternatively, the four digit date can be squeezed into the space of two digits by **encoding** it. Such methods, however, are non-standard and recoded data records may be incompatible with other systems. '**Interval**' techniques also keep the two digit format, and avoid the need to alter records, by defining a span of 'valid dates' (e.g. from 1920 to 2019). This interval may be fixed, or may advance by one year every year ('**sliding**'). This cannot handle dates over 100 years apart (28 years apart in some cases because of day-of-week calculations) and may also suffer from incompatibility problems. **Bridge programs** are software 'interpreters' which take over date processing from other programs, feeding back 'corrected' results into the system. In some cases, a system may be 'patched up' using bridge programs (e.g. while an entirely new system is purchased), but the programs are complex and error prone, and not a satisfactory long-term solution. The task is further complicated by the rather obvious **fixed deadline**. Two to three years is not long to correct the date change and test to make sure that the original problem is corrected without introducing new errors[2].

Box 1 MILLENNIUM COMPLIANCE: GENERAL PRINCIPLES

Approaches vary in detail, but share five key themes:

1. **Raise awareness throughout the organisation** of the existence and possible implications; in particular at Board level, as the issues may be fundamental to the survival of the organisation.
2. **Compile a complete inventory of computing and embedded systems,** from mainframes to PCs - including the 'human element' (e.g. form filling, etc.). Establish the exposure of the system to date change problems, especially 'mission critical' functions.
3. **Plan a solution** - decide whether to modify existing systems, replace with new 'millennium compliant' products, or take the opportunity to 'streamline' the business.
4. **Implement the plan.**
5. **Test the system**. This can be the most difficult and expensive stage, consuming over 50% of the overall effort and may take several years.

IT specialists and 'change consultants' have developed methods to help organisations to manage their date change projects. Within the overall approach described in **Box 1**, managers have to make key decisions - not only which technical approach to take, but whether to centre the project on in-house expertise (perhaps outsourcing some or all of the actual programming, often overseas), or to use a specialist IT consultancy. While automated software 'tools' for compiling inventories of IT resources, searching for date references, etc. are available, these will not avoid the need for significant human resources by either route.

Estimating costs is difficult. As a 'rule of thumb', programming costs about £1 per line of code changed. A typical medium sized company might rely on 15 systems (payroll, inventory, customer lists, etc.) which would use perhaps 6000 programs involving 12 million lines of code - it could cost £15M to carry out a complete Year 2000 compliance project, taking a dedicated team of 50 programmers almost three years. For a typical large organisation or Government Department with hundreds of millions of lines of code, costs could be over £100M. **The overall cost has been estimated as much as £20B for the UK, and £400B world-wide.** There is relatively little real experience on which to base firmer estimates, and they remain contentious.

Someone buying a car which might not start after 1 Jan 2000 would expect the manufacturer to remedy this. Of course, the computer industry is not the car industry, but the question can still be put whether vendors of

2. Each program change may affect on average, 8 other functions which need then to be checked. Making a large number of changes to an IT system without testing thoroughly may thus be as risky as doing nothing.

computers and software are 'putting their own houses in order'. Here, the picture is far from resolved.

Firstly, for **off-the-shelf systems**, put together by a customer from commercially available equipment and software (IBM or IBM-clone PCs running Microsoft, Lotus software etc.), **many new models of computer being produced and sold today still fail basic Year 2000 compliance tests[3].** Most **existing software is also vulnerable** and few software producers are correcting 'old' versions of their programs. Instead they will require customers to buy an upgrade to the newest version in order to gain millennium compliance. Yet most of the major software suppliers (IBM, ICL, Microsoft, etc.) have not yet released their full range of software in millennium compliant form, and do not expect to do so until some time in 1997. This will exacerbate existing trends for software to force premature obsolescence by being too 'big' to run on older computer hardware (e.g. many modern PCs cannot run the new Microsoft Windows 95 operating system), so many users will face the 'double whammy' of having to buy both new software and the computers to run it.

Turning to the larger **bespoke systems** (designed to meet a specification provided by the customer), future date compliance was often not made an explicit requirement in the purchase specification. Furthermore, many systems are modified in-house after purchase, so that there is great scope for dispute over who is liable for upgrading the system - even if the original supplier is still in business. There may not be time for negotiations over who shoulders the cost and customers may have little choice but to accept a compromise solution. This may be on the basis of 'best effort' rather than guaranteed performance.

Many will end up having to get on and do it themselves, creating a market for software 'patches' which work around the date change problems. Since the major software producers are not undertaking this themselves, the burden will fall on third parties, possibly producing a number of 'shareware' programs or more likely offering unproven services. Implementing such fixes will be difficult and devoid of guarantees.

NATIONAL & INTERNATIONAL ACTIVITY

The potential implications of the millennium date, the earlier failure of the main computer and software companies to compensate for it and the lack of awareness and preparation in industry, raise concerns in government circles worldwide. In the **USA**, the problem gained prominence in early 1995, and many organisations have Year 2000 compliance programmes in hand (e.g. New York Stock Exchange has completed its project, **after 7 years of effort at a cost of US$30M**). The House of Representatives Science Committee has an on-going inquiry into millennium compliance. The latest findings suggest that many US Government systems (including NASA!) may not meet the Year 2000 deadline.

In the UK, a survey of 535 public and private sector organisations (May 1995) found that while 70% of IT managers were fully aware of the problem, only 15% of senior managers were, and only 8% of organisations had conducted a full audit. Awareness began to grow in 1996 and there was an Adjournment Debate in the House of Commons in June in which the Minister for Science and Technology urged all IT users to tackle the problem. In July 1996 the DTI, CBI and the Computing Services and Software Association (CSSA) co-sponsored **Taskforce 2000** to raise awareness in the private sector[4]. As far as Government IT systems are concerned, in June 1996, the Deputy Prime Minister wrote to all Departments to establish their current positions. The Central Information Technology Unit (CITU) of the Cabinet Office has contracted the Central Communications and Telecommunications Agency (CCTA) to co-ordinate activities and CCTA has formed a 'Year 2000 Public Sector Group' to support departmental activities and provide a forum for sharing solutions.

Elsewhere in the world there is increasing activity, but many countries, including most in the EU, do not have any kind of national action programme in this field.

ISSUES

Catastrophic scenarios of Year 2000 failure are possible, but their probability is unknown. Indeed, some believe that incorrect date handling will be a nuisance rather than a catastrophe, and that many current vulnerabilities will be corrected as part of the normal cycle of maintenance and replacement. Resolving this uncertainty requires more experience from case studies on actual problems and their solution. Here, some organisations, such as British Telecom, view millennium compliance as a 'common good' issue and discuss it in public; others (including most of the UK financial sector) play their cards close to their chest. Despite this, some experience is accumulating (**Box 2** - next page).

Such cases suggest that the problem is sizeable but manageable given enough preparation time, and is within the annual IT budget of large companies. However for many organisations without their own IT development staff, Y2000 compliance may be more difficult to manage and in many organisations there is no 'new money' for Y2000 projects. Moreover, the consequences of an IT failure in modern business (whether in-house or in major customers or suppliers) can be grave and most experts urge organisations to

3. You can test your PC (make a backup first!) by setting the time and date to 11.58pm on 31 December, 1999, switching off and restarting after a few minutes. Many PCs reset to 4 January 1980.

4. The DTI is providing £70,000 for administration, and a further £100,000 for conferences and meetings. It is hoped that the Taskforce will become self-financing through commercial donations and subscriptions.

treat Y2000 as a business, not just a technical, problem[5]. Given the need to look outside for support, there are a growing number of software companies and IT consultancies offering millennium compliance services, from guide manuals (e.g. detailed analyses of the problem, case studies and solutions by Cambridge Market Intelligence, IBM, etc.) and 'software toolkits' to full audit and solution packages. It may be difficult to select from so many vendors and be confident of their abilities, and in response to such concerns, the CSSA and CCTA are compiling lists of compliance products and services.

The demand for reprogramming has revealed skills shortages- especially in the 'old' languages in legacy systems (e.g. COBOL), and IT project management. Experts predict that the cost of qualified staff may double every year as 2000 approaches, exacerbated by the re-programming requirement for European monetary union (whether the UK joins or not). Under such circumstances, many organisations are looking overseas (e.g.India), for the human resources needed. This raises concerns about security, and long term damage to the UK software industry if a culture of exporting programming develops.

There are other **national strategic interests** in privately owned systems. One concern is that 'safety-critical' systems (e.g. aircraft and air traffic control, nuclear power, emergency services) should be 'millennium compliant', another is the possibility of social and / or economic disruption arising from IT failures in benefit payment systems, banks, stockmarkets, etc. This leads some to suggest that Government needs to carry out its own strategic review to satisfy itself that adequate measures have been taken. One model to emulate might be the USA's research into national vulnerability to IT failures which has led to the concept of '***national strategic information assets***' - utilities, energy supply, emergency services, key transport infrastructure and the like. Once identified, this would provide a basis for national contingency planning for failure of IT systems.

Government Departments have responded to the Deputy Prime Minister's enquiries to the effect that the millennium date issue is under control. Assessing the situation is however complicated by trends in recent years whereby the central provision of IT purchasing and support has been devolved first to Departments and, in many cases out-sourced. Departments which have retained their IT expertise are some way down the path of auditing their systems and considering solutions, generally requiring complex negotiations with agencies and contractors - when the question becomes whether IT contractors have sufficient resources to complete the compliance work in time. Departments lacking internal expertise may find it more difficult to quantify the scale of the task and the CCTA / CITU are continuing to press the issue and offer guidance.

Box 2 EARLY LESSONS IN DATE COMPLIANCE

1. **Estimates vary widely**, for example an international financial company received quotes from software consultancies, ranging from £50M to £90M for complete compliance projects, compared with an internal estimate of £35M.
2. **It can be solved as part of routine maintenance**, for example, a UK clearing bank estimates the marginal cost of achieving millennium compliance at £5M, compared with an annual IT budget of nearly £500M. A large UK retailer estimates that all but 500 of the IBM PC clones embedded in its point of sale and stock control systems will have been replaced by 1999 through natural wastage.
3. **Some organisations have overestimated the cost**, for example a UK high street bank revised its original estimate of £90M down to £50M as its compliance project progressed.
4. **But others have underestimated**, for example by concentrating on mainframes and neglecting PCs, etc., ignoring 'lost opportunity' cost (e.g. an international photographic equipment supplier has suspended new IT development until the millennium issue has been resolved), or under-estimating the burden of testing.

Given the limited amount of time remaining and the experience of some companies that compliance projects can take many years, an obvious question is whether this issue **is being treated with a sufficient sense of urgency**? On the one hand, though starting later than the USA, the UK effort is ahead of many countries. On the other, a recent Taskforce 2000 conference in September found that none of the delegates (from clearing banks, insurance companies, etc.) was confident that their companies would be millennium compliant by 2000, and 10 (out of 300) 'knew' that they would not be.

The philosophy of Taskforce 2000 is that by targeting primarily the Boards of large business, the message will 'trickle down' as large businesses and Government place 'millennium compliance' conditions in contracts, purchases etc., and spread such conditions through supply chains to computer and software companies. Some argue that given the immediacy of the problem, there is not enough time for the trickle down approach to be effective and **a more active policy is required**. This underlies proposals by Members (e.g. Mr D. Atkinson 's 10-minute Rule Bill scheduled for presentation on 18 December 1996) to require companies to state whether their products are millennium compliant[6] at the time of sale. In addition, company auditors could include organisational exposure to Y2000 issues in their management reports to boards.

5. As illustrated only too vividly by the aftermath of the 'Bishopsgate bomb' attack on the City of London when companies without IT and data disaster recovery plans tended to go out of business.

6. A problem here is that here is no standard definition of 'millennium compliance'. The Information Technology Association of America has launched a 'Year 2000 Certification Program', which for a fee of US$4000 provides an independent assessment of an organisation's compliance programme (but not of its actual products). Analogous services are not available in the UK, but the British Standards Institute is writing a code of practice including a definition of the term 'millennium compliant'.