THE MILLENNIUM THREAT - AN UPDATE

- *How significant is the problem?*
- *Progress towards solutions*

Many computer systems may fail in transition to the Year 2000, because of the way they store and manipulate dates. Initiatives to address this problem in the public and private sectors have grown in the last year, but much remains to be done.

This note updates evidence on the potential scale of the 'date change problem' and the issues raised.

WHAT IS THE DATE CHANGE PROBLEM?

The date change problem is simply stated: many computer systems store the date as 2 digits - 76 for 1976, etc, and cannot cope with the Year 2000 becoming '00'. For example, the interval between 1976 and 2001 might be calculated 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 (e.g. **Table 1**). A more detailed description of the problem was given in POSTnote 89.

This apparently simple defect, however, turns out to have many facets (see **Box 1**), and may have far reaching and costly implications. Every computer system is potentially vulnerable, ranging from the 'mainframe' computers in large businesses, financial institutions and Government Departments to personal computers (PCs) on desktops and in computer networks. Furthermore, many computer 'chips' **embedded** in a wide range of electronic and mechanical devices, from telephone exchanges and fax machines to aircraft and security doors, also contain date functions and could potentially be affected.

Solving the date change problem suffers from a similar paradox, where the seemingly 'trivial' task of correcting computer programs and data described in **Box 1**, becomes much more challenging because of the size and complexity of computer systems.

CURRENT STATE OF PLAY

POSTnote 89 pointed out that someone buying a car which might not start after 1 Jan 2000 would expect the manufacturer to remedy this. In the computer industry, life is not so simple, and information from computer and software vendors on the status of their products is still incomplete. Part of this is because computers and software do not operate in isolation, and it is difficult to make definitive statements about the reliability of components when they are installed on a customer's system or used with other software packages. On the other hand, the competitiveness of the industry has not encouraged early anticipation or solution of the problem.

POST note **98** **June 1997**

Box 1 SOLVING THE DATE CHANGE PROBLEM

A number of date related errors have been discovered in computer programs. In addition to the 'obvious' problem of subtracting from '00', other problems arise in the way that '00' is interpreted (as 1900, 2000 or 'invalid'), calculating the day of the week, correctly treating 2000 as a leap year, etc. The consequences of such errors may range from generating subtly incorrect data to causing a whole system to 'crash'.

Erroneous programs can be corrected in several ways, but the three main techniqes are to **extend 2 digit years to 4 digits** throughout programs and data; to **start counting years part way through the century** so that, for example, dates between 1920 and 2019 can be represented using 2 digits; and to write **'bridge programs'** to take over date processing from other programs and feed back 'corrected' results. Each technique has merits (see POSTnote 89), but none of them escapes from the need to check millions of lines of code, written in any of over 2000 different programming languages with few standard methods of representing or processing dates. There are automated programming 'tools' to assist in this task, but these do not avoid the need for significant human resources.

A major challenge is the **project management** required for such 'root and branch' modification of computer systems. Approaches to this vary in detail, but share 5 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** - e.g. decide whether to modify existing systems or replace with new 'compliant' products.
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.

Perhaps the most important aspect of any 'millennium compliance' project is to consider the wider implications of the problem. It may not be sufficient to invest in fixing internal IT systems, if the failure of important suppliers or customers jeapordizes the core business. All organisations thus have to look at the problem from the viewpoint of their **whole** business - i.e. in-house operations **plus** customers, **plus** suppliers, if the scale of the problem is to be properly assessed.

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);**
- **The renewal period for HGV licences issued by the DVLA has been reduced from 7 years to 2 years due to Year 2000 problems;**
- **The Global Positioning System (GPS) for navigation using satellites must be reprogrammed to function correctly after August 1999;**
- **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 would not work on 29 February 1996 because it couldn't handle leap years.**

By now, however, most of the main companies are clarifying their position. Some, such as IBM took an early lead first in admitting the existence of the problem, and then in publishing the status of its products. Other major software producers have followed suit, but with so many different products and suppliers it is difficult to keep track of the latest developments. There is no single comprehensive 'guide', and the current situation has to be derived from looking at the latest information from individual manufacturers and independent testing organisations, which is mostly available only on the Internet's 'World Wide Web' (WWW). In reviewing the situation it is convenient to break down the problem into PCs and software, 'mainframes' and corporate systems, and embedded systems, although in the real world all of these may interact.

Personal Computers. It is still true that many new PCs currently on sale fail basic millennium compliance tests. Leading manufacturers, (e.g. ICL, IBM, Compaq) now sell millennium compliant machines and publish lists of models and serial number ranges giving the action required to 'fix' the date problem on PCs already sold. These range from software 'patches' for newer machines, to 'chip' replacements for older models, all of which will generally require some level of technical competence to carry out. But many other PCs are 'packaged' from the cheapest available components at the time, often by small, independent companies and shipped with little or no documentation. In such cases it is difficult to know what is 'inside the box', how to test its date handling and the appropriate solution for any problems detected.

As far as PC software is concerned, again the major vendors advertise the latest status of their products on the WWW. In most cases (Microsoft, IBM, etc.), the full product range is expected to be 'compliant' by the end of 1997, although it has become standard practice to*caveat* against errors introduced by other parts of the system (e.g. the PC's internal clock, or another program). Furthermore, with a few exceptions (e.g. Pegasus business software), most companies have stuck to the policy of not correcting 'old' versions of programs, obliging customers to buy a new version instead. Many users will have to upgrade or replace older PCs in order to be capable of running newer versions of programs (e.g. Microsoft's Windows 95 operating system is too 'big' to run on many existing PCs), thus increasing the cost of compliance further.

Corporate 'Mainframes'. The relationship between the mainframe computer industry and its clients is somewhat different to the PC market. Few systems are bought 'off the shelf', but rather they are customised from versatile 'core' packages, or built up from functional 'software libraries', to a specification provided by (or negotiated with) the customer. It is now generally accepted that there is **not** a significant problem with mainframe hardware, and that like the PC software industry, the commercial 'core' packages are expected to have been corrected by the end of 1997.

Because of the high level of customisation of mainframe software, and the 'legacy' of old code (see POSTnote 89) corrective action taken by the primary suppliers **does not solve most users' date change problems**. Neither, in most cases, can they expect the companies they used to configure and install their computer systems (if they are even still in business) to 'volunteer' solutions, since the suppliers question the extent of their liability, and there is little time to get involved in legal arguments. Organisations must thus take their own lead in addressing the date change problem, requiring a properly planned and executed 'compliance programme' (Box 1). Some may have sufficient internal resources to undertake such a project, but most have to look for outside assistance. Here, a growing number of companies are offering 'millennium compliance' services, from guide manuals, to software 'toolkits' to complete project management. There remains some concern about the quality of such services, and professional and trade associations (e.g. the British Computer Society (BCS) and Computing Services and Software Association (CSSA)) emphasise the need for high levels of professional conduct, and are compiling databases of their members offering date change and related services.

Last year, many industry observers were predicting that there would be a shortage of personnel with the required skills in modifying 'legacy' code (e.g. in the COBOL business programming language) and in IT project management. These concerns seem to be borne out: the market cost of qualified staff has doubled over the last 12 months. One consequence is that an increasing number of the major software houses have already fully committed their Y2000 compliance resources, and are not taking on any new work in this area. Equally, there is evidence that key staff with experience of date change projects are increasingly difficult to retain in the buoyant skills market.

Turning to the problem of **embedded systems**, it is much more difficult to assess industry response. Some embedded systems, e.g. in point-of-sale systems, are actually PCs in a different box, and so are under the purview of the computing industry, discussed above. But many others - ranging from simple timer chips to complex microprocessor controllers - are the products of manufacturing industry as a whole - automobiles, washing machines, bank vaults, and so on. There is thus no clear picture yet on how vulnerable such systems are, nor what measures manufacturers will be able to take to anticipate and respond to the problem.

NATIONAL & INTERNATIONAL ACTIVITY

The earlier POSTnote pointed out that the potential implications of the millennium date, the earlier failure of the main computer and software companies to compensate for it and lack of awareness and preparation in industry, had raised concerns worldwide.

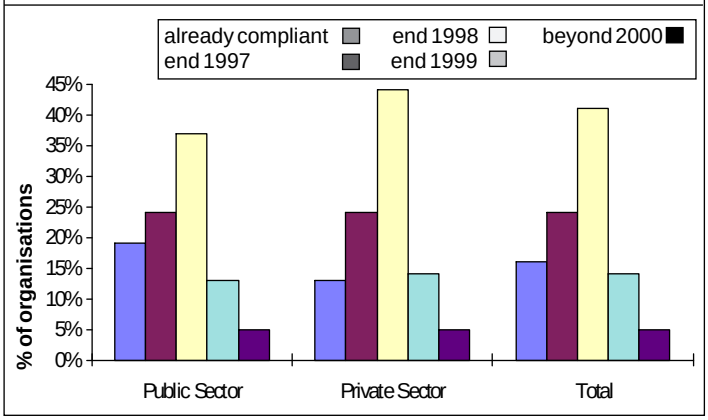
The USA is still leading in terms of the overall profile given to the date change issue. The on-going inquiry of the House of Representatives Science Commitee draws in expert opinion and helps raise awareness of the issues in the business community, among policy makers and in the media. Renovation of US government computer systems (mandated by Executive Order) is monitored by the Office of Management and Budget (OMB), which has set out a recommended timetable for work. The latest report (February 1997) suggests that several Federal agencies will come perilously close to the Year 2000 deadline; the State Department has already decided to limit renovation to its 'mission-critical' systems. OMB estimates that the total cost to the US Government will be US$2.3B, although there are other, much higher, estimates.

There have been a number of **developments in the UK**. As far as Government systems are concerned, the Central Information Technology Unit (CITU) has issued a 'Schedule for Action', requiring the completion of awareness and inventories, etc. by January 1997, fully costed and resourced plans by October 1997, and fully tested and 'ready' systems by January 1999. A report just released by the National Audit Office shows that 82% of public sector organisations are confident of keeping to this schedule (**Figure 1**), while most of the remainder plan to be ready in 1999. However, only 10% of public sector organisations had completed full audits, while 67% were partly completed. Estimates of the total cost are not available until this autumn.

The main national initiative to raise awareness in the private sector, Taskforce 2000, has established a firmer footing. The £70,000 funding from the DTI has been increased to £250,000 and a similar sum has been raised from industry. The original plan to target the Boards of large business has been supplemented, by DTI sending out 120,000 'information packs' to Small and Medium Enterprises (SMEs). No other country appears to have a comparable effort to mobilise its private sector to address the problem.

Another development in the UK was the introduction of a Private Member's Bill by Mr D.Atkinson MP under the 10-minute Rule. The "Companies (Millennium Computer Compliance)" Bill sought to amend the Companies Act (1985) to require audit of computer systems for millennium compliance and for the results, together with any proposed remedial action, to be stated in the annual report. In favour of such legislation, placing a statutory requirement on companies to consider their exposure to Y2000 issues would have a more direct effect than the 'informational' approach of Taskforce 2000. Such advantages, however, were balanced by concerns that the law would be difficult to apply, and additional regulation might be too inflexible, especially for SMEs. While the Bill received unanimous support (worldwide!) for raising the importance of the Y 2000 issue, the 3rd reading was not completed before the Dissolution. Whether or not such legislation would have been beneficial, it is generally accepted that any new legislation would now be too late to be much help. In any case, company auditors and regulators have started to discuss their role, e.g. with Taskforce 2000, and reporting of Y2000 exposure may well be realised more quickly through this route.

Figure 1 ANTICIPATED DATE OF COMPLIANCE



ISSUES

Nobody knows whether the Year 2000 will bring catastophic failures in computer systems, or whether there will just be a higher than usual level of irksome computer errors. Indeed, there are those who argue that the whole date change issue has been 'hyped' by the computer industry to generate business. Nevertheless, evidence is beginning to accrue that Y2000 compliance can be difficult and expensive to achieve, as illustrated in **Table 2** and **Box 2** (next page), where a number of companies are set to make substantial investments to address Y2000 issues. Assuming that the experience of such companies is indeed representative, estimates for the total global cost of Y2000 compliance are around £400B, while estimates for the UK range from around £10B to £30B.

So how well is the UK addressing the Year 2000 problem? As mentioned earlier, the Government sponsored Taskforce 2000 is unique in the world, and there are signs that it is succeeding in raising awareness in the

Table 2 SOME MAJOR COMPANIES THAT HAVE DECLARED YEAR 2000 PROGRAMME COST ESTIMATES

BT	£300M	Tesco	£40M	Natwest	£100M
BAT	£40M	Sainsbury	£70M	Barclays	£60M

Box 2 EARLY LESSONS IN DATE COMPLIANCE

1. **Many organisations initially underestimate the problem**, e.g. by concentrating on mainframes and neglecting PCs and embedded systems, ignoring 'lost opportunity' cost, or **under-estimating the burden of testing**.
2. **It can be solved as part of routine maintenance** - 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 will replace all but 500 of the PC s embedded in point of sale and stock control systems by 1999 through natural wastage.
3. **But time is running out** - most experts see 1997 as the 'watershed' year for taking action.
4. **Estimates of cost vary widely**, because of factors ranging from uncertainty in the magnitude of the technical problem to different accounting procedures.

business community, through wide media coverage. A survey for the DTI in Feb. 1997 showed that 85% of IT managers were fully aware of the problem (up from 70% in May 1996), while the proportion was 27% for senior managers (up from 15%). However, the proportion of organisations which had conducted a full audit of their computer systems had only risen from 8% to 9% since the earlier survey. With Government Departments, CITU's initiative has ensured that there is an awareness of the issue and that plans are in hand, a conclusion largely supported by the recent NAO report. However, the same report notes that 5% of organisations in the public and private sector will **not be ready** by 2000, and 14% plan to be ready by the end of 1999, which many observers argue is cutting it a bit fine. Even programmes that are scheduled to end before 1999 may drift much closer to the 2000 deadline.

Apart from the few large companies that are treating the date change problem as a 'common good' issue and discussing it in public (e.g. Table 2), most are still reticent and it is not obvious whether this is because they do not recognise the problem as important, or whether it reflects a desire to hide their vulnerability. Even organisations which are visibly taking action run the risk of 'analysis paralysis', where they may not leave sufficient time to implement **and test** programming changes, particularly in the light of the growing skills shortage discussed earlier.

Overall, there is feeling that 1997 is a 'watershed year' which will separate organisations that have made substantial progress towards renovating their systems from those that will simply not have enough time. Those which subsequently experience significant IT failures may find it difficult to survive, as illustrated all 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. Equally, organisations which are vunerable to instability in their supply chain may face difficulties, even if their own IT systems survive the transition.

Box 3 Y2000 COMPLIANCE - BSI

Year 2000 conformity shall mean that neither performance nor functionality is affected by dates prior to, during and after the year 2000. In particular:

- Rule 1. No value for current date will cause any interruption in operation.
- Rule 2. Date-based functionality must behave consistently for dates prior to, during and after year 2000.
- Rule 3. In all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules.
- Rule 4. Year 2000 must be recognized as a leap year.

In this context, there is concern that not enough attention is being given to **contingency planning** as discussed in POSTnote 89, either for individual organisations or at a national level. There is a tendency to place faith in the success of Y2000 compliance programmes, despite contrary experience from other large and complex IT projects. Given the added dangers of key staff being lured away and the imminence of the fixed deadline, not to mention the number of co-reliant organisations which may fail to take action at all, observers suggest that it would be wise to plan for some significant system failures.

Finally, it is widely accepted that the **legal implications** of the Year 2000 problem may be as extensive as the technical issues; for example in disputes over liability for the costs of Y2000 compliance programmes, product liability suits for failed systems, or claims for negligence against company directors for failing adequately to protect the interests of their investors.

One earlier problem was that 'millennium compliance' is difficult to interpret in isolation from the complete operational environment of an IT system. Here, model contractual terms (e.g. from the US Government and CCTA) are helpful, and the British Standards Institution recently issued a 'standard' definition of 'millennium compliance' (**Box 3**).

Whatever the technical outcome, observers predict that the legal bill may be 2-3 times the cost of fixing computer chips and programs. Thus, while legislation would now appear to have little to offer in delivering technical solutions to the Y2000 problem, it could have an important role in providing a framework for resolving legal disputes. Whether existing legislation is sufficient for this is still a matter of debate.