

# Y2K

**Prof. Simon Rogerson**

**Originally published as ETHcol in the IMIS Journal Volume 9  
No 2 (April 1999)**

As the year 2000 draws closer and closer organisations are becoming more frenetic in their efforts to ensure their computer systems are Y2K compliant. For example, around 30% of the 1999 IT budget of the top 100 European companies is being spent on Y2K compliance. There will be system crashes and there may be catastrophic outcomes resulting from these crashes. This is arguably the first world wide IT problem that strikes all sectors simultaneously. It presents a unique and unprecedented threat to our civilisation which has evolved into a computer-dependent society and an interdependent planet that is fragile and susceptible to a domino effect when a computer system crashes.

It is the size of the problem that poses the greatest threat not the complexity. There are 180 billion lines of program code to check and 1 billion embedded microchips to locate and check together resulting in an estimated 700,000 person years of work. Some claim that there is not enough time or people to complete this work but there has been progress. The latest annual survey of IT and operational directors by research organisation Benchmark Research reports that only 2% of organisations have done nothing, 27% have been given verbal assurances from suppliers, 40% have completed a systems compliance audit and 20% have replaced systems to ensure compliance. Some organisations have been addressing the problem for some time. For example, Sainsbury's Board gave their Y2K compliance project the highest priority back in 1995 and since then they have been working flat out to get their systems ready.

Clearly this is a major problem and one which puts society at risk. So who is to blame for this and should the IT industry accept some of the responsibility? There are many in the IT industry that argue no. They argue that because of limited memory and costly storage it made overwhelming economic sense at the time to use two digit dates. Furthermore software was not expected to last that long and so programmers did what was required to get a product up and working as fast as possible. The IT professionals of the day were simply ignorant of the potential problem at the turn of the millennium. And so two digit dates became another de facto standard within the IT industry. Indeed as late as 1995 microchips with two digit date procedures were still being shipped.

Is ignorance a defence in this case? What does it take for the IT industry to be culpable for its ignorance? The IT industry ought to have known that two digit date procedures would not work correctly beyond century boundaries. Indeed there were examples of this regarding people born in the previous century and "special measures" having to be incorporated to cater for these "exceptions". These warning signs should have alerted the IT industry to the millennium problem. It can be argued therefore that IT professionals

are directly culpable for their lack of knowledge resulting in the Y2K problem and hence are indirectly culpable for the resulting outcomes. Professionals should provide a higher order of care to the public and the IT industry is no exception. The public trust the IT industry to build reliable systems and it is questionable as to whether this trust has been abused in the Y2K context.

To be held responsible there must exist a causal condition and a mental condition. The former includes actions that were merely one significant causal factor among a number of others, while the latter includes unintended harm if the harm is brought about through negligence, carelessness or recklessness. If these definitions are accepted then there is a clear case of responsibility to answer because IT professionals acting in a careless and negligent manner were a significant causal factor of the Y2K problem. This careless and negligent manner included the lack of an integrated systems design approach, the lack of programming discipline and the lack of rigorous software engineering practices.

What has been the IT industry's response since the Y2K entry events of the creation and use of date algorithm routines? There were some early isolated reported concerns of the problem; in 1969/70 those working on systems in the UK in preparation for decimilisation identified problems with date field validation, in the USA in 1976 software engineers working on a Medicare system discovered potential fraud opportunities because of Y2K and in 1989, the American social security administration discovered that payment scheduling would not work beyond 1999 because of Y2K. Such incidents appear to have gone unheeded and generally there was a lack of willingness to tackle the problem at an early stage. In fact there seems to be a powerful dynamic of secrecy. Leaders do not wish to panic their citizens; employees do not wish to panic their bosses; corporations do not wish to panic their investors and lawyers do not want their clients to admit to anything. As the veil of secrecy thickens, the capacity for public discourse and shared participation in solution finding disappears. The IT industry appears to be party to such secrecy regarding Y2K.

Since the Y2K problem has been anticipated a vast compliance industry has sprung up with large financial returns being made. IT consultancy firms are showering their Y2K workers with sign-on bonuses, loyalty bonuses, project bonuses, and high salaries according to a recent survey. Obviously the provision of a quality service in this area is worthy of appropriate financial reward but has the IT industry in some way exploited the situation? For example, is it acceptable to offer Y2K software upgrades for sale rather than provide free patches for what are effectively faulty goods? Similarly is it acceptable that software tools that were not compliant were sold as late as 1997? Or is it acceptable that compression software that is suspect is shipped to customers? Organisations are concerned about their financial liability. It has been reported in the US that trade organisations are supporting a proposed new bill to limit liability of companies related to Y2K compliance. A recent news item reported that UK outsourcers were using termination clauses to avoid responsibility for Y2K crashes. Most contracts only have six or even three month notice periods so the impact on clients could be significant.

There are many serious questions to answer regarding the IT industry's role in creating the Y2K problem and its attitude in recent times to resolving this problem. A review of any of the codes of professional conduct in the industry suggests there might have been contraventions both in terms of attitude and practice. If so then the IT industry must have done something wrong, therefore it must be to blame, albeit in part, and therefore it can be held responsible. The industry should step forward, accept such responsibility and ensure that the risks of such world wide problems occurring again are minimised.

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson  
Director  
Centre for Computing and Social Responsibility  
Faculty of Computing Sciences and Engineering  
De Montfort University  
The Gateway  
Leicester  
LE1 9BH  
Tel:(+44) 116 257 7475  
Fax:(+44) 116 207 8159  
Email:<srog@dmu.ac.uk>  
Home Page: ( <http://www.ccsr.cse.dmu.ac.uk> )