Archive for historic interest:

The Year 2000 problem is gathering pace. By mid 1998 systems around the world were already beginning to fail - for example operations were cancelled for sick people in Britain because the computer system declared that vital supplies were out of stock. They were just out of date - or rather the computer thought they were. With expiry dates in the next millennium, the computer decided they were at least 100 years old.

So what is the real cost and can it be done in time? The answer is that no one knows what the cost will be, and it is already far too late. Most of the compliance year 2000 problems are in computer software written in Cobol, a language few know today. There is a global shortage of Cobol experts, and there are just too many lines of code to check. Year 2000 problems are often very subtle, and require extensive testing which itself takes many months, before any organisation can be certain that the risks have been eliminated.

How does the Y2K problem stack up: Kapoor and Parker's book "Leadership for Crisis Resolution - the Y2K Challenge" suggests the following:

Globally, initial software repairs $530bn, "bad fix" software repairs $50bn, testing $75bn, database repairs $454bn, hardware replacements $76bn, hardware upgrades $150bn, litigation and damages $300bn, total $1,635bn.

But are these figures real? A Congressional survey of the US government reported that the government alone would need to allocate $30bn just to sort out its own internal systems. The government spends $50bn a year on IT so the Y2K problems will eat up 20% of all government IT spending for the next three years.

The reality is that many corporations have now given up. Their boards took on trust naive estimates from senior executives, and are now worried about huge losses of business confidence, corporate image, consumer relations and profits, as well as big court settlements by people who can prove that their health or welfare was damaged as a direct result of failing to take Y2K action several years earlier.

So the pace has shifted to damage limitation, concentrating on the most vulnerable systems.

One solution is to start again from scratch, with new hardware and software, bearing in mind the doubling of computer power every 18 months and falling costs. However, new systems also need testing and integrating with the old.

Expect the markets to take year 2000 readiness into account when assessing the future of any company over the next two years, and year 2000 compliance to be a key agenda item in shareholders meetings for many industry sectors.

History will repeat itself - it is already with the Internet. Once again, pundits have described the future, while boards have buried their heads in the sand. Those in control are often scared of technology themselves, yet their businesses depend on it. What hope is there when many CEOs can't operate their own PCs with confidence and have never yet used the Internet on their own? They are being left behind, by a market which is developing seven times faster than any other we have ever seen. The internet is the biggest new market in human history, yet most companies can't see beyond a static web page plus e-mail.

If there is a lesson to be learned from Year 2000 problems it's this: if you don't take hold of the future, the future will take hold of you - and wipe you out.