Y2K—was it worth it?

1999 saw a flurry of activity and the expenditure of many billions of dollars worldwide to guard against the Y2K Bug. The media presented experts who predicted everything from 'the end of the world as we know it' to 'nothing is going to go wrong'. The general government and business position was that remediation work was well under way and that, no matter what happened, we were well prepared to protect the public.

Commonwealth and State/Territory Governments sought reports on remediation performance in the public sector and key business sectors. The negotiation of reporting requirements was usually undertaken in frank and open environments where information was shared freely. These meetings established good working relationships between government (including emergency managers) and key businesses as all were keenly interested in ensuring that, whatever problem existed, it was well understood and a clear solution was developed.

The actual event in Australia saw few formal reports of Y2K incidents. Anecdotal evidence suggests that many more incidents occurred but were not reported. Indeed, many companies were reported as saying that they would not report an incident unless they had to. They argued that they deal with hundreds of minor faults in service delivery every day and their contingency processes are well developed to cope with those without causing undue public concern.

With figures such as $12 billion being suggested as a national expenditure on Y2K, we should ask the question—'Was it worth it?' The truth, I suspect, is that we will never really know. Like any disaster, the challenges and benefits of Y2K extend beyond the immediate cause which, in this case, was information technology. The Y2K remediation process identified, and repaired, many technical problems. That process, however, was not limited to the technical. Government and businesses reviewed and tested contingency plans; many considered, and planned for, failures in utility supply, which after all can fail for reasons other than Y2K. In addition to business continuity planning, companies became more aware of the interdependency of utilities. Those utility companies gathered to gain a better understanding of that interdependency and how they might work in the event of a failure. In New Zealand, this work was commenced under the Lifelines Project—a concept that is yet to be fully embraced in Australia.

Y2K was also an exercise in public confidence with the media seeking to provide exciting stories. Companies tried not to give too much information prematurely with the main message being that remediation was under control and problems would not occur. Government tried not to become embroiled in discussions on the likely extent of the problem, preferring the message that no matter what happened, it was prepared.

The emergency management industry had to look at its own business continuity under Y2K conditions as well prepare for additional response to the consequences of Y2K incidents. It also played broader roles in gathering information on incidents, linking industry and government departments, and providing advice on contingency planning.

The reality of Y2K is that the public experienced no significant disruptions with only a few minor incidents being reported. Reports are not widely available on the results of control tests of original systems left to operate through Y2K. According to anecdotal evidence, some survived and some failed. Consequently, the questions such as 'was the exercise worth $12 billion' and 'was it all a hoax' are now being asked.

I suggest that the answers are not to be found in focussing on Y2K but the outcome of improved business continuity planning in Australia. Y2K was a threat, arguably it was poorly defined and people wanted answers before a full analysis could be completed. Nevertheless, Y2K was the catalyst for many activities, such as:

- improved awareness of the interdependency of lifelines;
- the establishment of networks for future cooperation between organizations
- the development or revision of business continuity plans within the private and public sectors
- the rationalisation of corporate IT, including a better understanding of the threats affecting it.

Was the expenditure on Y2K worth it? We may never know. But to lose the lessons of Y2K will be to ensure that it wasn't. The challenge to emergency managers, collectively, is to build on the partnerships established and the lessons learned to develop and promote the importance of planning and preparing for infrastructure failures beyond those that occur daily within a single industry.

Barry Stanton
Emergency Management Australia