The Millennium Bug

by Sedgwick Ltd

The Millennium Bug -otherwise known as the Year 2000, or Y2K problem.

The essence of the Y2K problem is that historically many computers, silicon chips and software were programmed with only two-digit date field to express the year.

Computers programmed in this manner will fail to recognise the change of millennium to 2000, and will either close down, read the date as 1900 or revert to 1980 (the birth date of DOS operating language).

The implications of Y2K noncompliance include a wide range of incidents where damage, financial loss and injury may result.

There is no "quick fix" that can be applied to the millennium problem. The multitude of computer languages and different systems in use, many of which have been custom modified, make solving the problem a complicated task.

The Millennium Bug problem is not simply one that effects mainframe computers. Personal computers, even models of the last few years and off the shelf and factory supplied software may not be Y2K compliant.

Although there is now widespread awareness of the issue by business, there has been surprising inertia in undertaking remedial action. Recent surveys suggest there will be a large number of companies that will not meet the deadline

A report by the Australian Institute of Company Directors released in December 1997 found that of 550 company directors surveyed, 47% had yet to begin action to address the issue.

Other recent reports support this finding. It has been estimated that 38% of Australian organisations are unlikely to find a solution in time.

The costs associated with the Y2K problem are impossible to quantify. Certainly the cost of compliance programs is significant and growing. It has been reported for example, that Telstra recently lifted its budget estimate to $500 million, five times the estimate released only three months earlier.

Organisations that do not address the millennium compliance issue now run the risk of going out of businesses, or, at least, incurring substantial costs and liabilities. The time-frame to fix the problem cannot be extended (as often happens with IT projects).

So how does this effect a legal practice?

There are three major areas we have identified as being particularly relevant to legal practices.

Whilst we have not contemplated an exhaustive list, in the following we have summarised some of the areas you may need to consider.

1) Administrative Functions affecting client records/files

This relates to your database management system, and the effect that a Y2K problem could have on your clients, creating a potential E & O situation, such as,

- corruption of diary system
- failure to manage statute of limitation issues
- missing court and response dates
- corruption of client files and information resulting in information going astray

2) First Party Business Risks

This area is where your client may not suffer a direct loss as a result of the corruption; but your business is affected due to:

- accounting system corrupted
- outstanding invoices not recognised
- paid accounts showing as outstanding
- client billing and time costing corrupted
- building and premises security and protection systems corrupted

3) Advice to Clients

This may be the most difficult area to manage. Potentially advice given in the past, before there was a wide awareness of the Y2K problem, and since awareness, may not have contemplated Y2K issues. Potential problems are:

- contracts drafted for client does not contain allowance for Y2K issues, resulting in your client suffering a loss and taking action against you.
- advice given on Y2K issues incorrect

What can you do?

Sedgwick have obtained advice from an independent consultant, PA Consulting, who advise that in their experience the principal challenges fall into two clear groups:

- scoping the magnitude of business risk arising from the Millennium Bug and communicating this to senior management in the organisation; and
- planning and implementing the route map to successful Millennium compliance including the organisation's interface with its supply chain and its customers.

PA Consulting recommends an approach comprising 5 stages:

1) Raise Awareness

Build an understanding of the implications of the Millennium Bug problem on the business and the urgency of addressing the issue.

2) Conduct Audit

Identify the extent of the potential problems along with where and how they exist, and their likely impacts on the business.

3) Decide Approach

Assess the merits of alternative courses of action for addressing the Millennium issue, decide the approach

continued over page

The Millennium Bug

by Sedgwick Ltd

continued from previous page

and plan the implementation.

4) Implement Solution

Put the implementation plan into action to fix the problem and track progress to enable any time slippage to be identified and resolved.

5) Perform Testing

Conduct extensive testing and reauditing to check that the actions have been successful.

The six critical success factors in a Millennium Compliance Programme are to:

- ensure that the programme is business-driven and involves senior management;
- recognise that the issue is unlike anything your organisation has done before;
- focus on the major business-critical exposure first;
- identify, secure and keep the resources that are going to fix the problem;
- generate a sense of urgency - the deadline cannot be moved backward;
- allow sufficient time and resources for the comprehensive testing.

The above is simply a review of the areas that may affect you and we recommend that you review all systems.

If you require any further information with respect to insurance issues and the Y2K problem, or would like to speak further with PC Consulting to obtain specific advice, please contact Cheryl Richardson at Sedgwick Ltd on 08 8211 7655

The article has been prepared by Sedgwick Ltd. The article is a general commentary and should not be used or relied upon as legal advice. You should not act or omit to act on the basis of the opinions, advice and other information contained in this article without first making your own inquiries as may be dictated by the particular circumstances of your case.

"The Millennium time bomb"

At the recent IPBA conference in Auckland, the Auckland Insurance Group organised a disaster scenario session on the implications for insurers and insured of failing to have computer systems year 2000 compliant.

The scenario for the session involved a Hong Kong company and its subsidiaries in seven jurisdictions: New Zealand, Australia, Taiwan, the Philippines, Singapore, the UK and the USA.

On 1 January 1999 the group, a highly successful canned food distribution business, is at serious risk. Canned food distributed to the seven jurisdictions for onward distibution to customers has been rejected as having its "sell by" date one year later. The computerised distribution system, being capable of reading the year 2000 only as "00", rejects consignments with a "sell by" date on or after 1 January 2000.

The subsidiaries in the region have guaranteed delivery dates to their customers in the festive season following New Year and approaching Chinese New Year. In many cases they now simply cannot deliver.
The head office in Hong Kong had sent our guidelines to the subsidiaries to ensure year 2000 compliance and the responses from the managing directors of each of the subsidiaries had been that they had consulted their IT suppliers and all was or would be well in time for 1 January 2000.

Each subsidiary has its own separate insurance arrangements. The subsidiaries each look to their All Risks Business Interruption policies. The managing directors of each subsidiary look to their Directors' and Officers' Liability policies. The subsidiaries' IT suppliers and advisers look to their Professional Liability policies.

Lawyers from each jurisdiction advised on the likely claims arising, whether or not the policies would cover the claims and why, according to the law of his or her own country.

Interesting differences arose. The analysis looked at the three likely heads of claim and whether these would in turn be covered by the three types of policy:

1 (a) The claims by the customers against the subsidiary - in all jurisdictions there was a main

continued page 23