

■ Lance B. Eliot, Feature Editor, Elliot & Associates

Y2K Late-Date Solution: Business Contingency Planning

Lance B. Eliot, Feature Editor

For many organizations that have waited to deal with their Year 2000 (Y2K) systems problem, time has just about run out. At this juncture, now well into 1999, it is unlikely that Y2K exposures that have been found can be completely fixed in time for the millennium change over. Unknown Y2K exposures that have not even been found yet are probably going to surface with insufficient time and manpower to fix in time.

Firms have but one reasonable choice now. Namely, dust off those disaster recovery plans (if they have any), and begin putting together a full-scale business contingency plan for the Y2K mess that will hit us all quite soon.

Indeed, even if you are one of the few organizations that has already completed your entire Y2K effort and feel secure that you are Y2K compliant, you still need to have a business contingency plan. Allow me a moment to explain why everyone needs a Y2K business contingency plan.

The Y2K problem is unlike any other kind of "traditional" disaster that we have ever faced in modern times. It is quite different from earthquakes, floods, fires, tornadoes, terrorist acts, and all other natural or man-made disaster events that we've faced in the past. Here's why.

Y2K will occur everywhere

The Y2K problem is found lurking in systems within your organization. Y2K is also found outside your organization in the businesses that your business depends upon for supplies. Y2K is also found in the businesses (your customers) that you pro-

vide with your products and services. Furthermore, Y2K is found at the local, state, and federal levels, and nearly all other countries and places on this planet.

Most natural or man-made disasters are relatively confined in a geographic sense. Therefore, a disaster recovery action often involves going outside the affected area in order to continue operating business in a normal fashion. Unfortunately, with the Y2K problem, there is no "outside" area. Y2K will be pervasive and inescapable.

Y2K will happen at the same point in time to all

Many people are surprised to learn that Y2K will happen not simply when the clock rolls over from 1999 to the year 2000, but

will also hit earlier in 1999 and later in 2000. In general, though, the bulk of the major problems will surface after the New Year change over.

In any case, the key point is that the Y2K problem will strike everyone in the same approxi-

mate time period. This is unlike most other disaster events that are typically scattered over time, striking one time and then another place at a different time, and so on (think of tornadoes touching down at different times around the world depending upon respective weather patterns due to the planet rotation).

Potential multiplicity of failures

Y2K can foul telecommunications, electrical power generation and distribution, oil and gas production and distribution, transportation systems such as aviation and

Failures in one part of the infrastructure can lead to failures in another part of the infrastructure, even if the other impacted part were strictly Y2K compliant in a narrow sense.



Lance B. Eliot

is president of *Elliot & Associates*, an information technology consulting organization based in Southern California. He holds a PhD in information systems, MBA and BS in computer science, and has also

earned the C.D.P., C.C.P., C.S.P., C.D.E., and C.I.S.A. certifications. He is the author of over 150 articles and columns, and the author or co-author of two books. He has served on the editorial boards of publications produced by the IEEE, ACM, DPMA, and similar organizations. Dr. Eliot has over ten years of experience in industry as a Chief Information Officer (CIO), Data Processing Manager, Systems Analyst, and Software Engineer.

Dr. Lance B. Eliot

Elliot & Associates

P.O. Box 30041

Long Beach, CA 90853-0041

email: LanceEliot@aol.com

shipping, and other infrastructure aspects of modern society. If a terrorist struck one piece of the infrastructure, the rest might be able to readily go on without it. But, in this case, we must anticipate that the pervasiveness of Y2K will mean that failures will be multiplied.

Y2K failures lead to other failures

Failures in one part of the infrastructure can lead to failures in another part of the infrastructure, even if the other impacted part were strictly Y2K compliant in a narrow sense. For example, if the power grid goes down, the telecommunications system will suffer without available power (even if all telecommunications systems were scrubbed of Y2K problems beforehand).

We know when, but not exactly how or how much

Predicting when an earthquake will hit is a hard thing to do. Knowing the consequences of a predicted size earthquake can be calculated and used to prepare for the consequences whenever it might occur.

Unfortunately, with Y2K we do not yet know how big the impact will be, nor how widespread it will really be. At least we do know when it will occur.

Part of the reason that we do not yet know the impact of Y2K is due to the fact that we are not sure where Y2K really lurks, and we are still working on preventing it from occurring at all.

An analogy might be made to the famous ship Titanic. If you knew that there were icebergs out in the water, but not sure where or how big, you could take action to try and prevent the Titanic from striking them and sinking. Thus, we can prevent or at least minimize the Y2K damages if we take appropriate action beforehand.

Business Contingency Planning

As the earlier points illustrate, organizations cannot assume that their conventional disaster recovery plans will be sufficient to cope with the Y2K problem.

Many information systems disaster recovery plans are narrowly focused on disruptions to Information Technology alone. In the case of Y2K, you must look beyond a technology focus and consider the enterprise-wide aspects of business disruptions.

- Suppose your major suppliers cannot deliver needed parts and supplies to your firm?
- Suppose your customers cannot get to the markets where you sell your goods?
- Suppose there are intermittent electrical power outages throughout the country?
- Suppose planes are delayed and reduced in the number of flights crossing the country?

These types of questions are not usually asked and answered in a typical information systems disaster recovery plan, nor in a general business recovery plan.

A recent quote by Jonathan Spalter, chairman of President Clinton's Council on International Y2K Issues, amplifies the point:

It is important to stress, however, that the Y2K problem is not a technical issue alone. World publics must be adequately informed not only about the scale and importance of the problem, but also about its nature so that the inevitable disruptions that will occur sometime, somewhere, in the first days of the year 2000 do not trigger worldwide trepidation, or even panic.

In working with firms to get ready for Y2K, I have developed a business contingency planning methodology that helps them consider the various impacts from Y2K, and help prepare a plan of action to cope with various levels of Y2K severity that might occur.

Topics that need to be addressed include:

- Develop a road map to potential break points.
- Review your insurance coverage capabilities.
- Establish Y2K disaster contacts in your lines-of-business worldwide.
- Identify the chain of command and control for when Y2K strikes.
- Set-up specialized "war rooms" for crucial collection and dissemination during Y2K crises.
- Have Y2K SWAT teams that are prepared to act when called upon.
- Do a threat analysis and vulnerability analysis.

- Develop various scenarios and test out your plans.

The development of the business contingency plan must be done with the awareness and blessing of the top executives of the firm. They must be made aware that Y2K can disrupt business processes, business resources, and the entire functioning of the organization.

As well, realize that people may react with concern for their own well being first, rather than the organization that they work for. If you assume that all employees will report to work to help get things back in order, you might be setting up your disaster recovery for a disaster. Employees may want to stay with their families, with their property, or may even be involuntarily prevented from coming into work due to other outages and infrastructure failures.

Conclusion

Let's be clear on my message in this column. I am not suggesting that we all get ready for the end of the world, nor am I trying to sell you on staying in a bunker and becoming a survivalist fanatic. What I am saying is that we do not really know how big a problem Y2K might be, and that as we get closer to the Y2K strike zone we will hopefully have a clearer picture.

Some economists have already predicted a worldwide economic recession due to Y2K. I remain concerned that we are not doing enough to identify and remedy Y2K problems right now, and worry that the Titanic is heading right for a big chunk of ice. I am hopeful that we will all take Y2K more seriously, including the development of an enterprise-wide business contingency plan to prepare for various possibilities, ranging from Y2K annoyance to Y2K knock out.

I guess we'll know soon enough. ■