NF99-402 Is Your Small Business Y2K OK?

Carol Thayer
University of Nebraska--Lincoln, cthayer1@unl.edu

NebFact

Published by Cooperative Extension, Institute of Agriculture and Natural Resources, University of Nebraska-Lincoln

Is Your Small Business Y2K OK?

Carol Thayer, Extension Small Scale Entrepreneurship Specialist

The Year 2000 (Y2K) problem started decades ago when early computers had meager processing power and memory and storage costs were much higher than today. In order to conserve space and money, programmers omitted the "19" in front of the year. The Year 2000 simply seemed too far off to worry about.

Data processing systems used in all types of businesses rely heavily on dates and date processing. If the computer code does not recognize that one date is greater than another, the computer may not be able to process properly and may produce erroneous results. The problem may put a business at risk because it can affect its cash flow, inventory, taxes, interest calculations, financial forecasting, customer relations and many other areas.

The worldwide problem not only affects mainframe computers and their programs, but also personal computers and every piece of hardware that contains a microchip. These are examples of items in your business that may be affected:

- Computer hardware and software
- Security systems
- Heating/cooling systems
- Fire alarms
- Employee records and attendance
- Mainframe applications
- Local area networks (LANs)
- Telephone systems
- Voicemail
- Office equipment (fax machines, copiers)
- Elevators

Every business is vulnerable. The ones that may be most affected are small companies that have automated some of their processes to remain competitive and those relying on extensive supply chains that might not be Y2K compliant.

Solving the Y2K problem is a business management problem. Deciding whether to spend the money, time and resources to address the Y2K problem is a business decision. The choices of what to fix and what to risk not fixing need careful consideration.

Compliance vs. Readiness

Before you can determine if your business is going to be ready for Y2K, consider the following definitions:

Compliance means that every system in your business can correctly handle date information in the Year 2000 without errors. Readiness means that your business may have some Year 2000 date issues, but they are not in critical areas and your business will be able to function correctly without interruption.

Y2K Project Steps

Now that you know that the Y2K problem can impact your business operation, it is important to develop a strategy to address the problem in small, manageable steps.

Step 1. Assessment. The first step is to conduct a comprehensive inventory of all the computer-based systems, components, service providers and hardware containing microchips that support your business. A good rule of thumb: if the device uses power, jot it down. In addition to internal items, you also will need to inventory your external relationships such as with utility and service companies, suppliers, and major customers. This inventory of potential problems will become the roadmap for bringing your business into Y2K compliance.

As part of the assessment phase, you will need to consider those devices that contain embedded chips that are date sensitive. These embedded chips contain software that is "burned into" the chip. Embedded devices control, monitor, or assist in the operation of machinery or equipment. Examples of equipment that may contain embedded devices include certain types of elevators, heating/cooling units, security and fire control systems, telephones, voicemail, credit card readers, fax machines, and copiers.

These questions can help you as you work through the assessment:

- Is the specific process critical and must the date problem be fixed or replaced to maintain systemwide functions?

- Should the date problem be fixed before 2000?

- Does the system allow for entry of a century indicator or four-digit year?

- Will the system operate differently depending on the day of the week?

- Can the system put things in order by date?

- Does the system allow you to retrieve things by date?

- Can the system perform date-based calculations?

- Does the system have a security feature that includes date checking?

- Can the old program or hardware be discarded?
- Are there enough resources to fix the problem and/or buy new hardware?
- What are the organizational and personal consequences if a system, process, or piece of equipment fails?

The "time horizon to failure" also should be considered as you assess your overall situation. Some systems may begin to fail prior to January 1, 2000 because they perform forecasting and future processing.

Step 2. Risk Status. After your inventory is complete, determine the individual item compliance. Contact vendors and ask for assurance statements from them or search vendor or manufacturer databases (many of which are available on-line) and download and save compliance information. You also may want to contact trade associations and other groups for additional compliance information.

Each entry on the inventory list should be ranked by how critical it is to your business. Here is one way of prioritizing risk:

- Life threatening - Failure could result in human death or injury;

- Mission critical - Failure could be disastrous to your business;

- Priority - Failure could have substantial impact on your business operation;

- Low Priority - Failure could result in trivial costs or minor inconveniences; and

- No risk - Used only for non-date-based functions.

Life threatening and mission critical systems, processes, and equipment items must be your first concern. Identify and evaluate items in these two categories as soon as possible to eliminate risk of failure.

Making any necessary replacements or modifications will then depend on the priorities you have set for your business. One of the biggest risks is an incomplete inventory which can cause whole processes to fail simply because something minor was left out.

Once you have determined the state of readiness for each system and component in your inventory, develop a strategy for addressing those systems that have to be fixed according to the priorities you have identified. There are several possible strategies: repair, replace, retire or use as is. Most businesses are taking a mixed approach to the Y2K problem. There is really no way to provide you with an accurate estimate as to how much it's going to cost to fix your Y2K problem, but it will cost something. Be prepared to spend money on things that are not normally part of your budgeting process.

Step 3. Planning. Y2K contingency planning can be approached like any other potential crisis or disaster. You will need to develop plans to ensure uninterrupted operation of the core business functions. This will include identifying steps to be followed if your business does experience a Y2K related problem.

While it is probably safe to say that you may not be 100 percent compliant by the Year 2000, what matters most is what you do between now and then to minimize the impact of any potential failures and how you handle the ones that slip through the cracks. This can be achieved by writing a *contingency*

plan that addresses "what if" situations. Contingency planning reduces risks, improves response times, improves financial viability, and reduces uncertainty.

A contingency plan for your business should:

1. Identify those systems too important to assume compliance and what should be done in case they fail;

2. Outline steps to address the failure of systems of moderate to significant risk where non-compliance is a possible or likely outcome;

3. Outline steps to address the failure of systems of low risk where compliance efforts will not be completed in time or even attempted; and

4. Be explicit where no action will be taken for systems of no significant risk or a low likelihood of failure.

Everything you do or that relies on someone or some entity outside your organization should be documented. If an outside agency says they are taking care of a Y2K-related issue that has the potential to impact your systems, *get it in writing*. In the unfortunate case where something goes wrong, it is important that you are able to demonstrate due diligence in your attempt to address the problem.

Step 4. Remediation. You have several options in addressing the problems you have identified:

- Retire - No longer needed or used.
- Renovate - Can be revised to handle 21st century dates.
- Replace - Can be replaced with a Year 2000 compliant system or device (if it cannot be fixed or if the fix would be too costly).
- Defer - Needs to be fixed or replaced, but not immediately.

It is important to realize that the remediated systems must be tested before they can be declared Y2K compliant. As you buy new computers, software systems, other hardware, or upgrade existing purchases/leased software systems, or develop new lines of business, remember that each new business component needs to be checked to ensure it is Y2K ready.

Warning: There are risks involved in rolling dates forward on computers. Some computer security systems keep track of the last time a user accessed a system and will revoke or deactivate that user's password if the system has not been accessed for a period of time. Rolling the date forward may cause user passwords to be deactivated. Datasets that should be retained may be marked as expired and written over. If you lease a software package and pay an annual fee to the vendor, rolling the date past the end of the lease may cause the software package to "freeze up" or generate error messages.

Whenever possible, testing should be conducted in a test environment. Also, you will need to be careful changing historical or backup files if you choose date expansion. Consult with your auditors and legal counsel before making modifications to historical or backup files or make certain critical files are backed up. Schedule the testing several months out if at all possible.

The IRS will allow businesses to deduct the dollar-for-dollar costs of dealing with the Y2K problem on one important condition: the costs must be incurred in the repair or conversion of existing software. Other software improvements require a three-year write-off.

Can you get insurance coverage for the Y2K problem? Because this is a foreseeable problem and any loss would not be as a result of an accident, you probably cannot get business interruption insurance. Review your existing coverage if a problem exists or seems likely to occur. Ask your insurance provider for specific information about your current coverage.

A *Conversion 2000:Y2K Self-Help Tool* has been developed to assist your business with assessment and planning. It is available in a CD or paper-based format. Each Nebraska Cooperative Extension Office has a copy of the CD. You may download the print version from the following WWW site: **http://y2khelp.nist.gov**.

Preparing for the Year 2000 problem is the key to ensuring survival of your business. Ignoring Y2K is a risk to the bottom line. Assessing and addressing risk is good management. If you, your customers, or your suppliers are not taking action, you are at risk. One problem anywhere in the supply chain will affect everyone in the chain.

Where to Get Help

Call the Y2K Help Center for Small Business at **1-800-Y2K-7557**; e-mail at y2khelp@nist.gov; or check out a website at http://y2khelp.nist.gov. Another option is to call your Cooperative Extension Office or the local Manufacturing Extension Program Center at **1-800-MEP-4MFG**.

Sources

Conversion 2000: Y2K, Developed by Iowa State University and The Manufacturing Extension Partnership. 1999.