

## 2. GETTING CONTROL OF THE PROBLEM — ASSESSING RISK

The first step in preparing for Y2K emergencies is to assess the threat. What is the nature of the hazard? What systems are at risk? How vulnerable are your communities and your emergency response agencies?

The planning process is similar to the one you use for other technological emergencies, but Y2K problems do have some unique features. They may affect:

- Many kinds of systems at the same time
- Many geographical areas — your jurisdiction and others — at the same time

And though the time of impact is predictable to a certain extent, it won't necessarily be at midnight on December 31, 1999.

### **How Widespread Is the Problem?**

To be blunt, the problem is pervasive. Just think of all the things we do every day that are now affected by computer systems.

These systems can be divided into two types: (1) *information technology (IT) systems* and (2) *systems that contain embedded chips*. IT systems include computer hardware and software — from the large computer systems that support large government agencies to the personal computers on people's desks. A wide variety of other devices and products contain embedded microprocessors (computer chips).

Some examples of IT systems are:

- Payroll systems
- Accounting and receivable systems
- Inventory systems
- Local or area-wide networks
- Management information systems
- Geographic information systems

Some examples of systems containing embedded chips are:

- Communications systems
- Traffic control and street light systems
- Building security and fire systems
- Elevators
- Automated heating and cooling systems
- Basic office equipment
- Electrical monitoring and distribution devices used by utility companies
- Biomedical equipment used in hospitals and nursing homes

These systems expand the scope of the Y2K problem. These devices and products have become essential, affecting nearly everything we do. Thousands of electrical and mechanical devices that we use in our private lives and during normal, day-to-day business are controlled by microprocessors. If these “invisible computers” fail, the effects could range from annoyance to disaster.

Many computers also are interconnected. A system may work fine by itself; but when it communicates with another system, it may experience Y2K problems.

Your best defense is to become aware of what can happen and prepare for it. Check the list of *Equipment and Systems to Check for Y2K Problems* on the next pages; it will help you start thinking about your communities' potential risk.

**Table 3. Equipment and Systems to Check for Y2K Problems**

Note: Read the list in its entirety because some equipment is multidepartmental. The list is not necessarily comprehensive; jurisdictions may find additional suspect equipment.

<b>Office Equipment</b>	_____ wireless communication systems (cellular phones, pagers)	_____ sprinkler/fountain systems
_____ telephone systems	_____ radar systems	_____ fuel dispensing systems (gas pumps)
_____ voice mail/answering machines	_____ security systems (door locks, safes, vaults)	_____ maintenance vehicles
_____ facsimile (fax) machines	_____ motion detectors	_____ other
_____ photocopiers	_____ parking ticket handheld devices	<b>Water and Wastewater Systems</b>
_____ printers	_____ police and fire computer-aided dispatch systems	_____ pump controller systems
_____ scanners	_____ surveillance cameras	_____ chlorine injection or other effluent disinfecting systems (ultraviolet lights)
_____ equipment w/ date stamps (video equipment, scales, time clocks)	_____ air traffic control systems	_____ lift station pump controllers
_____ personal computers	_____ fuel dispensing systems (gas pumps)	_____ telemetry systems
_____ laptop computers	_____ contingent systems (systems or functions that are operated by others, but on which the jurisdiction depends for its emergency response operations)	_____ vehicle computer systems
_____ personal digital assistants (PDAs)/handheld computers	_____ 911 systems	_____ equipment computer systems (mobile generators, mobile pumping equipment, construction equipment, maintenance and line cleaning equipment)
_____ wireless communication systems (pagers, cellular phones)	_____ public warning systems	_____ wastewater line televising equipment
_____ mailroom equipment	_____ other	_____ contingent systems or functions (systems or functions operated by others but on which the jurisdiction depends for its sewer/wastewater operations)
_____ other	<b>Public Works</b>	_____ other
<b>Emergency Response: Police and Fire Operations</b>	_____ traffic control systems	<b>Building Inspections</b>
_____ emergency response phone and dispatch systems	_____ flood/storm water control systems	_____ electrical generation and distribution
_____ global positioning systems (GPS) used to track vehicles	_____ electronic scales	_____ gas distribution
_____ EMT medical equipment (defibrillator; monitoring devices, blood analyzer)	_____ meters	_____ elevators, escalators, lifts
_____ breathalyzer	_____ handheld water meter readers	_____ building and premises security systems
_____ criminal records systems	_____ street maintenance systems	
_____ response vehicles, fire trucks, ambulances	_____ geographic information systems	
_____ two-way radio systems	_____ street lighting	

# Y2K

---

- \_\_\_\_\_ badge access systems
- \_\_\_\_\_ emergency systems (power generators, lights, HVAC systems)
- \_\_\_\_\_ engineering permits
- \_\_\_\_\_ engineering assessments reporting
- \_\_\_\_\_ fire control systems (alarms, sprinkler systems)
- \_\_\_\_\_ other

## **Administration/Finance**

- \_\_\_\_\_ utility billing systems
- \_\_\_\_\_ revenue systems (tracking of parking tickets, invoices, assessments, business licenses)
- \_\_\_\_\_ financial accounting systems
- \_\_\_\_\_ purchasing systems
- \_\_\_\_\_ payroll
- \_\_\_\_\_ tax collections
- \_\_\_\_\_ credit cards

## **Computer Network Resources**

- \_\_\_\_\_ routers
- \_\_\_\_\_ modems
- \_\_\_\_\_ switches
- \_\_\_\_\_ file servers
- \_\_\_\_\_ disk controllers and drivers
- \_\_\_\_\_ backup hardware and software
- \_\_\_\_\_ print servers
- \_\_\_\_\_ repeaters
- \_\_\_\_\_ uninterruptible power supplies and software
- \_\_\_\_\_ hubs
- \_\_\_\_\_ CD-ROM towers

## **Software**

- \_\_\_\_\_ operating system software
- \_\_\_\_\_ desktop publishing software
- \_\_\_\_\_ graphics software
- \_\_\_\_\_ desktop applications
- \_\_\_\_\_ optical character reading (OCR) software
- \_\_\_\_\_ virus scanning software
- \_\_\_\_\_ desktop utility software
- \_\_\_\_\_ custom software (desktop and network-based)
- \_\_\_\_\_ network operating software
- \_\_\_\_\_ network management software
- \_\_\_\_\_ client/server software
- \_\_\_\_\_ imaging software
- \_\_\_\_\_ other

## **Nursing Homes and Hospitals**

- \_\_\_\_\_ medical equipment
- \_\_\_\_\_ clinical records/patient information
- \_\_\_\_\_ accounts payable/receivable systems
- \_\_\_\_\_ HVAC systems
- \_\_\_\_\_ electronic billing system for Medicare and Medicaid
- \_\_\_\_\_ food suppliers
- \_\_\_\_\_ pharmaceutical suppliers
- \_\_\_\_\_ medical supply vendors
- \_\_\_\_\_ housekeeping supply vendors
- \_\_\_\_\_ other

## **Utilities**

- \_\_\_\_\_ energy control systems
- \_\_\_\_\_ power grid systems
- \_\_\_\_\_ power plants/stations
- \_\_\_\_\_ other

## **Interfaces**

- \_\_\_\_\_ banks
- \_\_\_\_\_ other governmental entities
- \_\_\_\_\_ automatic payroll
- \_\_\_\_\_ billing
- \_\_\_\_\_ dispatch
- \_\_\_\_\_ other

## **Service Providers**

- \_\_\_\_\_ banks
- \_\_\_\_\_ ATM machines
- \_\_\_\_\_ bonding firms
- \_\_\_\_\_ legal firms
- \_\_\_\_\_ appraisal companies
- \_\_\_\_\_ landfills
- \_\_\_\_\_ maintenance companies
- \_\_\_\_\_ trash collection companies
- \_\_\_\_\_ electric utilities
- \_\_\_\_\_ insurance providers
- \_\_\_\_\_ telecommunications companies
- \_\_\_\_\_ other

## **Food Storage and Distribution**

- \_\_\_\_\_ refrigerators
- \_\_\_\_\_ freezers
- \_\_\_\_\_ ice makers

## **Other**

- \_\_\_\_\_ railroad switching systems
- \_\_\_\_\_ robots
- \_\_\_\_\_ satellites
- \_\_\_\_\_ library cards
- \_\_\_\_\_ other

*Source: Adapted from A Year 2000 Action Guide, League of Minnesota Cities, 1998.*

## **How Can I Tell If I Have an Embedded Chip Product?**

Check to see if it:

- Has an LED (light-emitting diode) maintenance or operations panel with menu options
- Stores data for further use
- Has an internal clock
- Has controls for changing functions on the basis of times or dates
- Communicates with the user or operator, either visually or with sound
- Displays a time/date

## **What Can I Do About These Devices?**

Conduct an internal inventory to identify all items that may contain chip technology and all services that depend on them. Then try to check whether each product is Y2K compliant.

You should request letters certifying Y2K compliance from all of the applicable vendors. Be sure to insist that they describe the methods they used to determine compliance. If a vendor/supplier says its product is not compliant, develop a contingency plan to either replace the product or to deal with its failure.

## **When Will the Problem Strike?**

Most of the publicity about Y2K points to problems on January 1, 2000. But that is not the only critical date. Some experts predict a string of malfunctions throughout 1999 and 2000, rather than a single calamity. Why is this the case? Because programmers enter dates differently in different systems and products. Table 4 lists some of the dates that could cause problems and explains why.

**Table 4. Important Dates for Y2K**

December 31, 1999 – January 1, 2000	Last day of 1999, first day of 2000
Throughout 1999	One-year look-ahead date
April 9, 1999	May be mistaken for “end of file” code
September 9, 1999	May be mistaken for “end of file” code
February 29, 2000 – March 1, 2000	Uncommon leap year
December 31, 2000	366th day of uncommon leap year
August 22, 1999	Rollover date for GPS systems
July 1, 1999 to October 1, 1999 (various months)	Start of government fiscal year 2000
January 10, 2000	First date in the year 2000 with 7 digits
October 10, 2000	First date in the year 2000 with 8 digits

As an emergency manager, you also must monitor and respond to Y2K problems that could occur days or weeks after January 1, 2000. Some incidents might initially seem unimportant, but they could turn into threats to public safety and health. For example, a medical facility’s treatment equipment might be working; but if its payroll system were to be disrupted for very long, the facility might have to close. Or a power plant in one location might be operational but have to shut down after a few weeks if Y2K disruptions elsewhere were to stop fuel shipments.

Publications and web sites devoted to testing systems for Y2K compliance list other dates that should be included in a complete system test. See the references listed under “Resources for Testing Your Systems” in *Section 3*.

## Vulnerability Analysis

Potential disruptions caused by Y2K problems are similar to other technological emergencies, so you can apply FEMA's all-hazards planning guidance (State and Local Guide 101, *Guide for All-Hazard Emergency Operations Planning*, September, 1996) to Y2K problems as well.

In addition, FEMA 141, *Emergency Management Guide for Business and Industry* (October 1993) includes a section on planning for technological emergencies. You may want to consult the whole guide. See *Section 5* for information about getting a copy.

The initial focus of contingency planning should be on those systems that you identify as most critical to your agencies' operations and to your communities. Vulnerability analysis will help you identify these systems. Here are some excerpts on vulnerability analysis from FEMA 141 to help you prepare.

Use the *Vulnerability Analysis Chart* (Table 5) to assess the probability and potential impact of Y2K emergencies. The process entails identifying potential problems, assigning probabilities, estimating impacts, and assessing resources, using a numerical system. The lower the score, the better.

## Directions for Using the Vulnerability Analysis Chart

### List Potential System Failures

In the first column of the chart, list the Y2K failures that could affect you, such as:

- Safety system failure
- Telecommunications failure
- Computer system failure
- Power failure
- Heating/cooling system failure
- Emergency notification system failure

### □ **Estimate Probability**

In the Probability column, rate the likelihood of each emergency's occurrence. Judging the likelihood of Y2K failures is difficult in large systems like communications or transportation. Even the experts disagree. But you don't have to be highly precise. Use a simple scale of 1 to 5, with 1 as the lowest probability and 5 as the highest. This is a subjective consideration, but it is still useful.

### □ **Assess the Potential Human Impact**

In your work as an emergency manager, this step is critical. Analyze the potential impact that each emergency could have on people, such as the possibility of death or injury. Assign a rating in the Human Impact column of the Vulnerability Analysis Chart. Use a 1 to 5 scale, with 1 as the lowest impact and 5 as the highest. In this area, for example, 1 might equal discomfort, and 5 a loss of life or limb.

### □ **Assess the Potential Property Impact**

Consider the potential for property losses and damage. Again, assign a rating in the Property Impact column, 1 being the lowest and 5 being the highest. Consider:

- Cost to replace
- Cost for temporary replacement
- Cost to repair

### □ **Assess the Potential Business Impact**

Assign a rating in the Business Impact column. Again, 1 is the lowest, and 5 is the highest. Assess the impact of:

- Business interruption
- Employees unable to report to work
- Imposition of penalties or legal costs
- Interruption of critical supplies or services

### □ **Assess Internal and External Resources**

Next assess your resources and ability to respond. Consider each potential emergency from beginning to end and each resource that would be needed to respond. Assign a number to your internal and external resources. The lower the number, the better. Ask yourself:

- Do we have the needed resources and capabilities to respond?
- Will external resources be able to respond to us for this emergency as quickly as we may need them. Or will they have other higher priority areas to serve?

If the answers to these two questions are yes, move to the next assessment. If the answers are no, identify what can be done to correct the problem. For example, you may need to:

- Develop additional emergency procedures
- Conduct additional training
- Acquire additional equipment
- Establish or modify mutual aid agreements
- Establish agreements with specialized contractors

### □ **Add the Columns**

Add the numbers for each emergency. The lower the number, the better. While this is a subjective rating, comparing the numbers will help you determine planning and resource priorities.

