Y2K SERVICE CONTINUITY PLAN FOR EMERGENCY SERVICES DEPARTMENTS

Executive Analysis of Fire Service Operations
In Emergency Management

BY: Randy Templeton, Battalion Chief
Austin Fire Department
Austin, TX

An applied research project submitted to the National Fire Academy as part of the
Executive Fire Officer Program
May 1999

ABSTRACT

The problem before the Austin Fire Department (AFD) was to develop an appropriate Service Continuation Plan (SCP) to meet the challenge of the Year 2000 (Y2K) date changeover. The purpose of this applied research project was to survey and gauge the fire service's Y2K service continuity planning effort to date and investigate whether other plans exist which may be used as a template or planning guide. Procedures used included literature review, survey of two independent fire service groups, telephone follow up, review of other planning templates and participation on a citywide task force.

The researcher chose the action research model as most appropriate for this project. The final research project output was a comprehensive, usable Y2K SCP. In developing this Plan, the researcher considered the following questions:

1) What is the likelihood of significant infrastructure problems associated with Y2K?
2) What are the expectations of others in the fire service community concerning Y2K problem significance and call volume?
3) Are other fire departments developing mitigation strategies and service continuation plans? If so, are any useful when developing a planning model for AFD?
4) What are the likely problems associated with any expected infrastructure collapse, and how can preparation be made in advance?

The researcher expected to find widespread complacency toward the Y2K problem within the fire service, with few fire departments engaged in serious preparation for what had the potential to be a life- and career-altering event. The research results confirmed that, although 94% have a Mitigation Plan, only 34% of respondents have a SCP in place or in process, indicating that most fire departments are not fully prepared for what may occur with the New Year. The researcher recommends that fire service organizations begin an immediate industry-wide education and motivation effort to encourage emergency services departments to prepare for events if mitigation efforts fall short.

TABLE OF CONTENTS

INTRODUCTION

"Why Y2K?"

General Dwight D. Eisenhower once said, "In preparing for battle I have always found that plans are useless, but planning is essential." Our culture has become accustomed to dealing with threats from all types of man-made and natural disasters. Most city, county and state governments have developed response plans and procedures to deal with what have become commonplace, though tragic, events.

Yet, with the possible exception of Noah's flood, never in recorded history has our nation and the entire world faced a catastrophic disaster like the one that is possible with the turn of the century. The Y2K problem stands out as unique among disaster types in at least four ways:

- It is a scheduled event. All technologically advanced nations will face the same issues and infrastructure failures within a 24-hour period. There is no delaying or avoiding the consequences of the march of time.
- It is global in its scope. With most disasters, localized distress can be relieved from outside sources as people and jurisdictions cooperate. Resources are shifted from unaffected areas to areas of need. Y2K will be a simultaneous event, and each local government will be on their own to mitigate its effects.
- It is insidious. Until the very hour of the stroke of midnight January 1, 2000, and the days immediately following, the full effect of pre-incident mitigation efforts will not be known.
- It is steeped in myth, mystery and intrigue. The new millennium is the long-anticipated event around which some sects and cults build end-of-the-world so-called prophecies. Others may use this time as an opportunity to attempt to induce panic and terror. The media has charged still others with attempting to stir panic for personal gain in order to sell books or survival supplies. Regardless of the motivation of others, these events will likely directly impact the lives and jobs of emergency workers.

With effects estimates ranging from “a blip on the screen” to “catastrophic meltdown and the end of our society as we know it,” it is difficult to know how much preparation for Y2K is appropriate. What preparation is prudent, and when does preparation cross the line into paranoia? There are several historical/traditional reasons for pessimism:

1) The Information Technology (IT) industry has a consistent track record for being substantially behind schedule and over budget for normal projects over the past 40 years.

2) Approximately 70% of U.S. organizations are at SEI level-1, which means they have no process for reliably predicting schedules and budgets for projects.

3) Year 2000 projects are the largest and most complex projects undertaken by most organizations.

4) Even if they do finish on time, the IT industry has a consistent track record of delivering buggy software—on average, one defect per function point after testing. (Cutter Consortium, 1998)

Until the problems fully present, preparation efforts will have to rely on the professional judgment of emergency services planners. Administrators are understandably reluctant to spend large sums of money to prepare for an event that may not live up to its advance billing. For this reason the process of hammering out planning assumptions and expectations is at the heart of this and all other contingency planning processes.

Emergency workers may be facing a prolonged challenge the likes of which they have never experienced. Equally apparent is that if events unfold as direly as some believe no amount of preparation will be enough. Or, as others insist, fire fighters will pass a quiet shift, barely noticing anything out of the ordinary in the way of call volume and nature.

With the Y2K contingency planning problem, as with the Y2K programming problem, the “fixes” are not as troublesome as the management issues and decisions associated with them. Prerequisite to all other planning decisions are comprehensive planning assumptions. Secondary, but closely related, are the

costs associated with preparation. Third, some very significant human resource issues present when making mandatory staffing decisions for the "party of the century" holiday.

Purpose of This Project

The problem before the Austin Fire Department (AFD) was to develop an appropriate Service Continuation Plan (SCP) to meet the challenge of Y2K. The purpose of this applied research project was to survey and gauge the fire service's Y2K service continuity planning effort to date and investigate whether other plans exist which may be used as a template or planning guide. The researcher also performed a review of literature to find out what current information is available about Y2K preparations. With the assembled information, and with the planning assumptions and Technical Compliance Plan provided by the Austin 2000 task force (comprised of representatives of all City of Austin departments), the task was to evaluate the potential problems, situations, and response levels of AFD for the defined critical period and other minor Y2K dates. From this evaluation the researcher was expected to project the staffing, resource and equipment needs. The projections were then assembled in a comprehensive SCP for use by AFD during the upcoming Y2K event(s).

The researcher chose the action research model as most appropriate for this project. The final research project output was to be a comprehensive, usable Y2K Service Continuation Plan (hereafter, the Plan, or SCP). Developing this Plan, the researcher considered the following questions:

1) What is the likelihood of significant infrastructure problems associated with Y2K?
2) What are the expectations of others in the Fire Service community concerning Y2K problem significance and call volume?
3) Are other fire departments developing mitigation strategies and service continuation plans? If so, are these useful when developing a planning model for AFD?
4) What are the likely problems associated with any expected infrastructure collapse, and how can preparation be made in advance?

The researcher expected to find widespread ignorance, complacency, or both toward the Y2K problem within the fire service. He had arrived at this anecdotal conclusion based on numerous conversations with a cross section of both local and national fire service personnel. Many individuals did not seem to understand the technical threats, nor had they done intentional research. They therefore tended to dismiss the Y2K issue as the invention of extremists with "axes to grind" or products to sell. The student expected to find few fire departments engaged in serious preparation for what had the potential to be a life- and career-altering event.

BACKGROUND AND SIGNIFICANCE

The Planning Problem

The complete "big picture" implications of Y2K for emergency services departments are no clearer that for the rest of society. There are, however, steps in the planning process that can assist emergency services with preparing for this and any other disaster. The first is to clarify responder's role in a chaotic environment, followed closely by the adoption of reasoned and sound planning assumptions.

Philosophically speaking, the *fundamental* task of all emergency services is to bring *order* out of *chaos*. Other tasks include mitigating the potential harm and/or the prevention of chaos before it occurs. The presence of an efficient, well-trained emergency response system is psychologically soothing to citizens because they can be confident that there are professionals who will help to restore order when situations are uncontrolled (e.g., the fire service declares fires, when they are out, "under control").

An emergency by definition is an urgent event that is, or is perceived to be, threatening to life or property. It is axiomatic that fires, medical emergencies, entrapments, and wide range of other emergencies introduce disorder into the routine lives of citizens. Fire departments exist to deal with chaotic situations in their many forms for which most citizens are ill equipped. For that reason citizens will look to

emergency services personnel to help normalize their life should Y2K cause infrastructure disruptions, especially if the event meets the worst expectations.

Cities, by training and equipping fire fighters (as well as other emergency responders), and by maintaining other essential aspects of a response system, dedicate resources directed at restoring societal order. The corollary of this process is preserving life and property (the Mission of many fire departments, including AFD). The form of the particular out-of-control situation determines the appropriate agency response. This emergency system forms a social "safety net" of sorts. It is essential for a successful system to be continuously scanning the environment for potential threats and designing appropriate responses. It is our job to plan for life's extremes. In this context, it is of diminished importance that the actual threat of Y2K is undefined, since the potential threat is fairly clear: unbridled chaos that could threaten our very societal foundations. The fire service shares with the military the distinction that both are charged with preparing for the unthinkable on a daily basis. For many, Y2K represents just that.

When considering the appropriateness of preparation levels, emergency planners must consider the potential consequences of the worst possible scenario compared to what is most likely to occur. These then are evaluated and contrasted in the light of the risks and costs. This process is seldom scientific, but it can be systematic. And what may be taking an acceptable risk to some is to others an act of irresponsibility. If the consequences of failure to act or plan on the part of public administrators are great enough, the failure may rise to the level of tortuous, or even criminal.

In addition to the technical and managerial problems presented, underlying issues of global interconnectedness and the uncertainty of exactly what will happen are two complicating factors that make the emergency service planners' job extremely complex. These factors also make adopting planning assumptions (the "driver" of all good planning processes) often an extension of the planner's own internal continuum of optimism-versus-pessimism, or hope-versus-fatalism.

Few professionals are comfortable outside of the mainstream of thought and practice. What

agency administrator, after all, is willing to publicly predict the end of our civilization? The current theme among mainstream Y2K writers and officials dealing with the challenge is that our institutions and infrastructure will be ready. There will be problems, yes, but for the most part we have the problem "licked." (There are notable exceptions, with some very knowledgeable writers maintaining serious-to-devastating eventualities.) Y2K is unique among planning events in that there is, by its nature, introduced in the planner an internal conflict, even a subtle feeling of guilt, by assuming and planning for the worst. Following the mainstream, however, raises the question of whether or not by so doing the fire service forfeits its ordained mission of being the safety net, prepared whatever situation presents.

The issues at stake are extremely complex and the consequences of being wrong (conservative or extreme) are high. They are so complex and so high that they tend to force us psychologically to cling tenaciously to the "middle of the road." The issues are so complex and the costs so high, in fact, that we may be many years into the next century before the last of the problems are solved and the final lawsuits are settled. One very popular spin off of the "Y2K industry" is seminars for attorneys concerning how to sue for Y2K problems. It is projected to be one of the richest "gold mines" for tort litigation in the history of civil jurisprudence because it was foreseeable and preventable. (Thorpe, 1998, pg. 6) Some experts believe that we may never fully recover from the chaos caused by a simultaneous global malfunction of networked computer systems and infrastructure.

The Technical Problem

Understanding the Y2K technical problem begins with understanding the computer jargon. In "computerese," Y2K is an abbreviation for Year 2000. In simple terms, the Y2K problem, or "millennium bug" as it is often called, is likely to cause computers programs and chips that have not been remediated to malfunction or fail when the date rolls over to 01/01/2000. These malfunctions or failures may take various forms, including (but not limited to) shutting down automated programs, failure of chip-reliant systems, erroneous messages, computations and other data.

At the heart of the problem is how a computer processes information, specifically, how it uses date field data. When presented with the transition of 99 to 00 in the date field, most computer programs cannot handle the disparity. The date January 01, 2000 can be misinterpreted in one of 3 ways:

1999 December 31 23:59:59 + 1 second = undefined date and time

This would affect all scheduled activities undertaken by the system. If the resulting date and time are earlier than that which existed prior to the transition, date comparisons could give negative results. This would produce runtime errors and system failures. Systems which rely on 'day of the week' or 'month of the year' information could also malfunction, locking out security doors, freezing office tower elevators or bank vaults for the 'weekend', or switching from heating to air conditioning.

1999 December 31 23:59:59 + 1 second = 1900 January 01 00:00:00

This transition could produce errors of the type described for an undefined date and time. In addition, any operation performing date comparisons could fail. There may be problems with some routines suffering from 'division by zero' problems.

1999 December 31 23:59:59 + 1 second = default date 00:00:00

Such a transition could result in any of the problems outlined above, depending on the default date. Often the computer assumes that "00" denotes the year 1900 AD. Other programs default to the year they were first designed. (Sells, 1998, p. 16)

In order to fix and clean a computer program, all of the two-digit date fields must be found and corrected to four digits. It is a tedious process that must proceed line-by-line until completed. Not one single date field may be missed, or the programmer runs the risk of re-contaminating the program. Some tools have become available to help speed the process. An average program contains one date field every fifty lines of code. Multiplied by the trillions of lines of code in existence, the scope of the total mitigation problem worldwide is staggering.

Repairing the date fields in software is not the only problem. Some computer experts believe that

the embedded chip systems present at least as much, if not more challenge. These systems consist of tiny read-only-memory (ROM) microchips that have some controlling or measuring function in a myriad of items. These include (but are not limited to) electrical generation systems, vehicles, water pumping systems, other utility services (e.g., natural gas or propane supply), oil drilling, transportation systems (e.g., airplanes, trains, ships, etc.), valves, and appliances. Virtually every electrical tool, implement, appliance, or vehicle produced in the last 15 years has from one to hundreds of these chips. It is estimated that there are between 25-50 billion in service. Of these, failure rate estimates range from 5%-15% with Y2K date rollover. (Missler, 1998) No one is able to accurately predict which 5%-15% will be affected.

There are several potential problems associated with embedded system affecting correction of the Y2K problem. First, embedded chips are often extremely expensive to replace--up to $15,000 each. Second, many systems are in inaccessible locations and cannot be replaced (e.g., satellites or oil drilling heads in the deepest parts of the North Sea). Third, sometimes the clock/calendar function of a chip is not evident. Many chips are “boiler plate” design, with standard built-in functions. But not all of the capabilities in the chip are used in its application. Usually this fact means that they have a clock/calendar function integral to the mechanism itself, but not evident in the purpose of the machinery or apparatus. These may fail without warning with the date rollover, and be very difficult to find. (Missler, 1998)

The Managerial Problem

It is apparent in conversation that most people familiar with Y2k issues misunderstand the actual nature of the problem, believing its solution to be of a technical or programming nature. This misunderstanding has lead to an unjustified optimism on the part of many that just before the stroke of midnight, Bill Gates (of Microsoft Corporation) or some computer nerd working out of his or garage will provide the “magic bullet” that proves to be the ultimate fix. This optimism is at best an expression of confidence in the ingenuity of business and its ability to meet any challenge. It is at worst a dangerous naivete that can lead to inaction while waiting on someone else to act.

Though there certainly are major technical components, the overarching problem is managerial. The managerial issues are almost overwhelming, complicated by a fixed deadline and the fact that business and government have delayed response until it was nearly too late to be successful. Managerial issues include determining and managing the (1) scope, (2) cost, (3) timing and scheduling of remediation efforts, and, (4) the complexity and interconnectedness of systems. These issues will require difficult management choices and innovative solutions.

1) Scope

Finding and correcting the date fields in trillions of lines of code is no mean task, but it is not even the most difficult or time-consuming portion. Two-digit date fields occur on average in every 50 lines of code. These must be searched out and, once found, corrected with a four-digit date field. Recently some remediation programs have been introduced to tell the computer to fix itself (the so-called “magic bullet”). Some of these tools have proven useful, but they remain, at best, an aid. These also only help with the software programming.

Problems are seldom linear, and the Y2K fix is no exception. A computer is nothing more than an engine that runs software applications. Since the inception of computing over 500 programming languages have been employed (Thorpe, 1998, pg. 9). Most of these are arcane and have fallen into disuse. Others are still used, but have been changed and patched over the course of 25-30 years. Many of the original programmers have retired or died (Thorpe, 1998, pg. 9). Programming more accurately resembles art than science, and programmers often take full artistic license. Additionally, few of the programming patches have accompanying documentation or mapping that would facilitate making corrections.

There are also other problems to correct besides the two-digit date field. A favorite trick of programmers in the past was to insert a code in the programming string which, when activated, was useful for stopping runaway applications. Many programmers used “9999” as that shutdown code. It is not clear precisely what will happen on September 9, 1999, but many experts feel that the date 9/9/99 when inserted

into software applications will activate the code, shutting them down automatically, and may not restart. Even if they do restart, many programs will cause permanent damage or loss of data with even a temporary shutdown.

Another problem is that Year 2000 is a leap year, but many systems will assume that it is not. Calendar rules designate year numbers ending in 00 are not leap years unless divisible by 400. Many program designers unfamiliar with calendaring rules (established by Papal decree in 1582 AD) will miss this important subtlety and their programs will therefore not compute the date accurately (February 28, 2000 + 1 day).

These "other problems" have created dates other than 01/01/2000 which have the potential to crash computers. These minor Y2K dates beginning in April 1999 and continuing through October 2000. Any of these could cause problems, the cumulative effect of which may result in chaos:

- April 9, 1999 — 99th day of the year, could affect systems using Julian dates.
- July 1, 1999 — New fiscal year for some government agencies.
- Aug. 22, 1999 — Roll-over date for Global Positioning System
- Sept. 9, 1999 — Auto stop code for some programs (9/9/99)
- Oct. 1, 1999 — Beginning of fiscal year
- Jan. 10, 2000 — First date requiring the use of seven digits
- Feb. 29, 2000 — A non-standard leap year day
- Oct. 10, 2000 — First date requiring the use of 8 digits
- Dec. 31, 2000 — Another leap year problem—366th day of the year

2) Cost

Remediation is the process of retiring, replacing or modifying software or devices (e.g., items dependent on ROM chips, or programmable logic controllers) that have been determined through risk assessment to be subject to failure during a Y2K event. The problem of the cost of remediation projects is

managerial, not technical. The cost has already been staggering to business and government, and it continues to grow.

Fortune 500 companies, for example, estimate that Y2K projects will cost approximately $11 billion. (Thorpe and Bramblette, 1998, pg. 7) Edward Yardeni, Chief Economist for Deutsche Banks Securities, Inc., has examined the Securities and Exchange Commission disclosure statements and has concluded that the 400 publicly traded companies will spend $29 billion fixing computer systems. (Regan, 1998, pg. 19) Capers Jones, Chief Scientist with Artemis Management Systems, estimates that when all of the dust settles, the total bill will be in the neighborhood of $90.4 billion. (Regan, 1998, pg. 19) Current Gartner Group estimates of global expenditures to fix the problem are on the order of $1 to $2 trillion, which is about 3%-5% on average of every country's gross domestic product. (Gershwin, pg. 1) Employing lawyers and paying Y2K damages has been estimated at $1-$3 *trillion*. (Christiansen, pg. 2)

The silver lining is that many organizations are taking a hard look at their information systems, and replacement of older systems should have a positive impact in the long run. The down side is that spending money to fix Y2k problems diverts money from other projects. (Christiansen, pg. 2)

3) Timing and Scheduling

Most of the remediation work must be done on systems and programs in daily use in business and government. Some of the work can be accomplished while programs are in use by creating partitions on a drive and remediating or testing in the partitioned portion. However, a large portion must be done after hours or off-line. Scheduling the work can be a management challenge.

Once an organization's systems are determined to be compliant, all other inter-dependent systems must be checked as well. The only way to be certain of compliance is test, test again, and verify. (Thorpe, 1998, pg. 6) Testing must be done realistically and in concert with all interactive systems. Testing and certification are a significant management challenge and should be the most time-consuming portion of the remediation process. Programming repairs are notorious for introducing as many problems as they fix and

often result in new bugs worse than the original program. So many organizations have waited too long to begin remediation to be able to give appropriate attention to testing and certification. That very important portion of the task is likely to be left incomplete. Many systems will not be properly tested until field-tested by the date rollover.

4) Complexity and Interconnectedness

A "system" is defined as "a collection of organized, interrelated processes." (McCrackin, 1995, pg. 6) Dependency relationships are everywhere in our society and between societies. Electrical power is a classical example: without it most of our familiar structures shut down. Other examples are communications, other utilities, transportation, and commodities. Failure in one or more sectors has ripple effects throughout the system. The managerial problem is to understand, anticipate and map all of the potential exposures that come through interconnectedness and dependency. Once mapped or modeled, remediation can be begun. A parallel effort must be commissioned to develop contingency or continuity plans in case projects cannot be finished in time or unanticipated failures occur.

Not only must systems be remediated and tested, they must be tested in conjunction with all of the programs with which they interact. If any are missed, the agency risks system failure and even re-infection.

Another dependency problem occurs with "just in time" (JIT) warehousing of parts for manufacturing. Since JIT scheduling saves money by reducing the stock that must be kept on hand, any interruption of the normal flow of parts can result in a shutdown in production. Manufacturers and emergency service providers must not only be concerned of the compliance of their own equipment, but also their suppliers.

The Social Problem: Security, Terrorism and Panic

Even if all technical problems are remediated in the United States, the social problems worldwide cannot be. It is widely accepted that many countries will not be prepared, including many in Latin America, Africa, and Asia. Japan, Mexico, China, Germany and Taiwan have been named in Senate testimony as

countries falling desperately behind—as much as nine months to two years. (The Economist, 1998, pg. 1) Oil producers Venezuela and Saudi Arabia are thought to be 12-18 months behind schedule. The concern is that Y2K-caused computer collapse will trigger widespread economic collapse, leading to civil unrest and terroristic activities. (Entous, 1999, pp. 1-2) If the oil producing capacity of Venezuela and Saudi Arabia are diminished, the effect on the United States will likely be immediate and severe.

The fact that Y2K will fall in the middle of winter for Northern Hemisphere nations raises humanitarian concerns should heating sources be affected. Economic problems and food shortages, coupled with already difficult conditions in countries like Russia and Honduras, could cause major upheaval, and even backlash against the United States.

The Department of Defense (DOD) is preparing to head off other national security issues. The DOD will sometime this fall complete a Joint Center for Year 2000 Strategic Stability located at Peterson Air Force Base, Colorado. The purpose is to "give [Russia] confidence that nothing 'funny' is going on." (Verton, 1999, pg. 1) It is widely recognized that Russians could interpret warning screens blacking out from lack of power as a precursor to nuclear attack. According to Sen. Christopher Dodd (Connecticut), failure to include the Russians in a Joint Center… would be "the ultimate form of Russian roulette." (Verton, 1999, pg. 1)

In the opinion of many of the current writers, the gravest problem facing America at home is widespread panic and overreaction. Few things motivate people more to take action than does fear—and there may be reason to fear. Withdrawal of funds from banks, hoarding food and water, and the purchase of weapons to protect the former are seen as likely consequences of the crisis preparation, especially as the fourth quarter of the year approaches. The problem may be compounded as some of the optimistic estimates for correction approach the reality of the deadline, and public statements begin to project more of a sense of urgency. Even if no crisis materializes, certain segments of the economy are likely to suffer through the first quarter or half of next year as hoarders use up stored supplies.

The symbolic meaning of the new millennium cannot be ignored. Some sects and cults are founded on the premise that the end of the world is upon us. To what degree these will act with violence to make their own prophesies come true is unknown. But it is likely on at least a regional basis. Other groups have as their mission the destruction of what they deem an oppressive system of government. What better way to erode the public's confidence than to prove by terrorist act that their government cannot protect them. By introducing more chaos into the system already struggling to maintain stability, terrorists may try to introduce the factor that pushes American society over the edge, and accomplishes their anarchistic objectives. To a terrorist, Y2K may spell opportunity.

The "Street" Problem (The Effects on Emergency Service)

Emergency services should anticipate the possibility of significant problems associated with Y2K and a moderate-to-heavy increase in emergency call volume. The increase in calls for assistance could be associated with any or all of the following reasons:

1) Medical Calls

Stress induced by the anticipation of problems may cause conditions associated with high blood pressure, anxiety, or depression. There may be a number of suicides. Pacemakers may malfunction, causing cardiac arrhythmia. Vehicle entrapments and medical calls associated with auto accidents may increase since there is likely to be many people driving and an increase in alcoholic beverage consumption. Hospital and home health equipment may malfunction, requiring fire fighter intervention. Carbon monoxide could be a problem if citizens are forced to use alternative heating appliances.

2) Fire Calls

If power is lost, an increase in structure fires is likely due to the use of candles or fuel-fired lanterns. In the months leading up to and immediately following Y2K, what fires do occur may be more severe (especially in residential structures) if owners have stockpiled fuel supplies (e.g., gasoline or diesel, Coleman fuel, propane, etc.). Microprocessors and sensors designed to regulate safety conditions in

equipment may fail or cause overheating and safety system failure. Enunciator equipment for fire alarm systems may not work, resulting in the failure to remotely detect fires in their incipient phase. If conditions result in civil unrest, arson is likely. An increase in arson cases is often the result of an economic recession, as is possible with Y2K.

3) Terrorist Event

Segments of society reportedly view the millennium as an opportunity to seek publicity for their cause through terrorism. Others may seek to de-stabilize the government. Any event of this nature would be designed to damage structures or cause casualties, and could stress an already busy emergency response system.

4) Hazmat

Many safety and containment systems in industry are automated using embedded chips. Unanticipated failure of these could trigger a hazmat emergency.

5) Aircraft Emergencies

Airplanes, both private and commercial, and heavily dependent on computer chips. Airborne craft could experience Y2K-related emergencies, as could the air traffic control system.

6) Grass/Brush Fires

Fireworks are a major problem as ignition sources for wildland fires. Emergency services often staff extra units for fireworks calls during the New Year's holiday. Fireworks manufacturers report that they are quadrupling their inventories in anticipation of a banner sales year. The increased use may result in increased call volume for brush fires, and consequently structure fires if allowed to spread.

7) Alarm Activations

The failure of embedded chips may cause false alarm activations in many fire detection or suppression systems. Fire units investigate each alarm activation (depending on local policy), and often stand by until the owner or key holder can arrive. This stand by policy is an example of one that may need

to be temporarily suspended due to call volume and service demand.

8) Elevator Entrapment

Emergency services units assist persons entrapped in elevators when they malfunction. This is a possible outcome due to potential failures of embedded chips in the elevators of high rise buildings.

9) Other Power Outage Emergencies

Widespread power outages would likely result in calls for assistance for persons using certain medical equipment. These incidents are often true emergencies, since prolonged deprivation of the equipment can be life threatening for these individuals. Also, when the power has been off for a time and comes back on there are often emergencies resulting from electric stoves or other heating equipment left in the "on" position.

10) Weather Related

The Y2K holiday occurs during the winter, and cold weather emergencies and winter storms are a possibility for which emergency services must be prepared. This will be especially problematic if electrical or natural gas services are lost and home heating mechanisms fail. Deaths of homeless persons and burst water pipes could be collateral damage from low temperatures.

Of course, call volume is not the only problem associated with Y2K. If problems are truly serious, as would be the case with regional-or-larger power outages, or long-term disruption in other infrastructure systems, emergency services departments will likely have human resource issues. For example, fire fighters, police officers, and paramedics are also fathers, mothers, and children to the victims. Will these employees remain at work if their families are in need? Will volunteers respond to others' call for assistance when their own families are in discomfort or danger? Departments must have a plan that includes care for the families of service providers.

Other staffing issues will likely be problematic. Will the department cancel scheduled leave over the holiday billed as the party of the millennium? Can the organization afford the increased overtime costs,

particularly in the light of a possible impending recession and accompanying loss of tax revenue? Who will be considered essential personnel, and what job classifications will be non-essential? Will the Emergency Operations Center (EOC) be staffed, with whom, and how long? Will the department establish a Department Operations Center (DOC)? Will reserve units be staffed?

As the potential scenario is extrapolated through the planning process, departments should develop a plan for the "worst case", including feeding employees, heating buildings, providing drinking water, obtaining water for fire fighting, restoring problematic communications, providing and fueling generators, to name a few. Even if departments do not take the step of spending the funds to purchase provisions, a plan should be in place to anticipate the needs. This process will of necessity make the plan a living document, subject to change, amendment, and refinement right up to the last minute.

Emergency Management Issues: The Planning Process

This applied research project is the result of the researcher's interest in emergency planning following his taking the National Fire Academy's *Executive Analysis of Fire Service Operations in Emergency Management* (EAFSOEM) course. The problems presented by Y2K present an excellent opportunity to exercise the process and implement the steps in the following major unit topics of the course:

1) Unit 3: The Incident Command System (ICS)

The AFD has been using the Incident Command System (ICS) for approximately sixteen years. The SCP was developed in the context of ICS as the organizational management tool. All AFD personnel and many of the other emergency response agency personnel have been trained to the advanced level in the Standardized Emergency Management System model.

2) Unit 4: Community Risk Assessment

The AFD, in conjunction with all other City Departments, conducted a Community Risk Assessment for Y2K. Risk assessment prepares for an emergency in three distinct phases: prevent, event, and post-event (FEMA/USFA/NFA-EAFSOEM-SM Student Manual, 1997, pg. SM4-6). The prevent phase of risk

assessment was incorporated into a Technical Compliance Plan (TCP), and was the first step in the overall planning process. The TCP was prepared by a task force of subject matter experts from different sections and divisions within the Department. The effort addressed the three components of a model Community Risk Assessment:

1) Assessment of the risks that task the fire and rescue agency beyond normal capacities, called critical risks.

2) Assessment of the risks' effects on the community and the agency.

3) Development of the strategies that involve the groups and agencies that would respond to the risk. (FEMA/USFA/NFA-EAFSOEM-SM Student Manual, 1997, pg. SM4-4)

The TCP inventoried current equipment and evaluated both the risk of failure, remediation required, and expected timelines to completion of the task. The event and post-event phase of the risk assessment process was incorporated into the SCP prepared by the researcher and approved by the AFD Command Staff.

3) Unit 5: Incident Documentation

Incident documentation addressed in the SCP included procedures for completion of standard forms and other documentation in the event normal documentation processes are interrupted. The need for documentation with the probability of litigation was also stressed. Of vital importance was the documented evidence that AFD had explored vulnerabilities and had made plans for correcting them.

4) Unit 6: Capability Assessment

Portions of the Capability Assessment were addressed in both the TCP and the SCP. For example, critical emergency response and support services were identified, and vulnerabilities explored. Cooperative agreements were reviewed, and found to be likely of little value in this type of regional or extra-local emergency. Assumptions were made about service demands and AFD's capability to meet those demands with staffing and equipment. Other outside sources of resources were considered and explored

where internal supplies were not sufficient, or where a back up source was desirable.

5) Unit 7: Media Relations

Provisions for good media relations were included in the SCP, including identifying trained personnel who will serve as Public Information Officers for the critical period. Also identified was the need to reassure and educate the public as the New Year approaches, with the limitations of public panic and anxiety being the major focus.

6) Unit 8: Damage assessment

Damage assessment is essential to Y2K planning because of the unknown factors going into the event. The bridge between potential problems and the actual situation is the process of assessment. The SCP contains a systematic process for assessing and reporting damage or malfunction by fire units to the EOC. Because the effects of computer malfunctions may be spotty or regional, fire apparatus will need to drive their response territory to properly make assessments. The information will then be assembled in the EOC, and a comprehensive damage assessment picture will emerge.

7) Unit 9: Emergency Operations Center (EOC)

The EOC will be the central coordinating authority for the City of Austin and the AFD. The SCP addresses staffing of the EOC, duration of operation, and certain elements of its organizational structure. The relationship between field units and the EOC is described. Resource coordination will be the primary challenge of the EOC staff, and the command group for the incident citywide will be headquartered there.

REVIEW OF THE LITERATURE

Current literature concerning the Y2K event can be found in abundance. There are multiple web sites devoted to the spread of information concerning the problem. Facts and their interpretation can be found from both ends of the spectrum of future event expectations. Most of the web sites, magazine and

newspaper articles, books and tape sources were produced within the past two years.

How the Problem Developed

The language of computers is the worldwide language. The technical problem arises from the fact that in the 1960's when computers and computer languages were being initially developed, all date fields were represented by using two digits for the month, two for the day, and two for the year. One of the early programming languages used in mainframe computers was COBOL, whose earliest versions did not support the entry of years in a four-digit format. (Wierzbicki (Ed.), 1998, pg. 4)

The reason for this system designers' choice and common practice of the industry is the topic of some debate. Many familiar with programming practices claim that the method became convention because storage space was extremely expensive before modern methods of production dramatically lowered the cost of stored memory. "The Gartner Group, a consultancy in Connecticut, estimates that one megabyte of magnetic disk storage space in 1965 was $765, compared to $0.75 today, and perhaps as little as $0.34 in 2000." (The Economist, 1998, pg. 2) Others assert that it was not the cost of memory, but sloppy programming by lazy programmers that is the cause of our current crisis (Pierce, 1998, pg. 88). Still others insist that it is hypocritical to blame programmers for scripting date fields according to common business practice. (Cairncross (Ed.), 1998, pg. 2) Besides, few programmers believed that the programming that was being written in the 60's would still be with us nearly forty years later.

So, in a sense, the problem stems from a failure to adjust by an industry that has experienced tremendous growth over 30 years. What was originally a necessary programming approach has never been eliminated as newer equipment and greater capabilities became available. (Wierzbicki (Ed.), 1998, pg. 3) Much of the original mainframe programming exists, buried under layer after layer of patches. "In many cases the Y2K problem was intentionally carried over to the present as new programs were written using old specifications and algorithms to avoid reformatting database information." (Wierzbicki (Ed.), 1998, pg. 5)

General Progress Report

One of the early pioneers sounding the Y2k warning was Peter de Jager. He testified before the House of Representatives Science Committee on May 14, 1996, and titled his presentation *Unjustified Optimism*. Mr. de Jager cited statistical studies showing that programming projects larger than 100,000 function points in size (about 12,500,000 lines of Cobol code) are delivered on time only 14% of the time. (de Jager, 1996, pg.1) At this point in time, organizations still in the early phases of remediation should consider a triage approach and attempt to complete only mission critical systems. (Graham,1998, pg. 26)

Another Y2K expert, Capers Jones, Chief Scientist for Artemis Management Systems in Burlington, Mass, indicates that he believes that at this point (January 1999) a 95% repair is the "best case" scenario. In the 95% scenario, he believes:

[1] Electric power, water, shipment of goods would be disrupted for about three days;

[2] Approximately 330,000 people would lose their jobs, at least temporarily.

[3] The cost to repair the systems and lawsuits would be about $90.4 billion. (Regan, 1999, pg. 19)

But Jones believes that the most likely scenario will be an 85% remediated scenario, and the likely results would include:

[1] About 2.2 million people could lose their jobs.

[2] The unemployment rate could rise 2.2%.

[3] Some 2,500 businesses and 275,000 individuals could declare bankruptcy.

[4] About 15% of the nation's homes and businesses would be without power for five days and without telephones for three days.

[5] Air, road, sea and rail transportation could be interrupted for days, or even weeks.

[6] Stocks would lose 10% of their value in early 2000.

[7] The cost of replacing computers, software equipment and lawsuits could top $497 billion. (Regan, 1999, pg. 19)

Federal Progress Report

On March 31, 1999, *Cable News Network* (CNN) reported on a General Accounting Office (GAO) report that the White House and nearly half of the federal agencies missed the internal deadline imposed by the President for the federal remediation effort to be finished and for testing of systems to begin. The same report said that 13 of the 24 major government departments have brought "100% of their critical systems into Y2K compliance," and 10 of the 11 remaining have achieved 85% completion. (CNN, 1999, pg. 1) However, much of the government has yet to test. And while the federal government claims to be 92% compliant, the Dietrich points out the invalidity of claiming to be compliant prior to testing, comparing it to "…testing a parachute without pulling the ripcord." (Diederich, 1999, pg.1) The GAO expressed great concern for three departments: Federal Aviation Administration, Health and Human Services, and Department of Defense. (CNN, 1999, pg. 1-2)

Following the release of the GAO report, on March 2, 1999, Senator Robert Bennett (Utah) and Senator Christopher Dodd (Connecticut), two members of the Senate Special Committee on the Year 2000, commented on it. Bennett said that Americans can expect "…a bump in the road…that it will not be crippling. We do not expect this to be…the end of the world as we know it." (CNN, 1999, pg.1) Both Senators expressed concern that the health care industry is lagging behind. The most concern, however, is with international preparations, as most countries are lagging far behind in their Y2K preparations. (CNN, pg. 3)

In a March 31, 1999, press release concerning the federal government's Y2K conversion efforts, President's Council on Year 2000 Conversion Chair John A. Koshinen and Office of Management and Budget Deputy Director for Management G. Edward DeSeve praised federal employees for working diligently and making extraordinary progress in the past year. They also outlined the four key priorities that Federal agencies will be pursuing in the 275 days left before the New Year:

[1] Completion of Y2K work on remaining mission critical systems and on other Federal systems;

[2] Cooperative efforts to end-to-end test and demonstrate Y2K readiness of Federal programs with states and other partners critical to the administration of those programs;

[3] Completing and testing *business continuity and contingency plans as insurance* against disruptions to Federal service delivery and operations from Y2K-related failures; and,

[4] Continued outreach to non-Federal organizations in the public and private sector to *promote action on the problem and contingency planning.* [emphasis added] (Koshinen and DeSeve, 1999, pg. 1-2)

State and Local Progress Report

According to the Gartner 90% of the computer applications will fail and computers will crash if not corrected. The night of December 31, 1999, may be "volatile for PSAPs [Public Safety Answering Points] around the world," according to *9-1-1 Magazine* (Larson, 1998, pg. 44). *The New York Times* even ran an editorial on August 2, 1998, which advised its readers to prepare for the worst. (Porlier, 1998, pg. 18) "What was a technical and management issue is now one of public safety and quality of life." (Porlier, 1998, pg. 21)

In their press interview of March 2, 1999, Senators Bennett and Dodd expressed concern that 13 states and the District of Columbia are lagging behind. (CNN, 1999, pg. 3) Also, according to a press release by the National Association of Counties (NACo) dated December 8, 1998, only half of the nation's counties have developed a strategic plan for dealing with Y2K problems. The NACo survey showed that exactly half of the 500 counties surveyed had a plan. Of the 16 counties with a population of over 500,000, all but one had a plan in place. Only one-third indicated that they had completed the task, while 41% said that they were halfway completed. The survey indicated that the counties need another $1.7 billion to reach full compliance. (NACo, 1998, pg. 1)

Cities seem to be in a better position to complete the task. According to a January 1999 survey conducted and released by the U.S. Conference of Mayors, 97% of the respondents have a citywide plan to

address Y2K issues. Of the 220 cities surveyed (population 30,000 or more), however, only 54% had a contingency plan for unexpected failures. The cities reported spending a total of $90.8 million, and listed their priorities (in order of frequency) as emergency response, management information systems, general government administration, police department, utilities, taxation, and finance. The survey further reported that cities are have the most difficulty finding and fixing embedded systems. (U.S. Conference of Mayors, 1999, pg. 1)

Contingency Planning

Power, communications, water, transportation and other essential services are looking less-than-assured the closer they are examined. Experts assert that the problem cannot and will not be solved in time. "Recovery planners must act now to be sure that their organizations have planned effectively for failure." (Campbell, 1998, pg. 25) Although preparing for failure is not a natural, in the face of almost 100% certainty that Y2K projects will encounter failure, preparations need to be made. (Freeman, 1998, pg. 24)

"The intensity of the problems ahead is largely dependent by what actions are taken in the interim on a local basis." (Porlier, 1998, pg. 20) "The concerns and preparation for municipal governments are more complex even than corporate issues, since most will be tasked with coordinating damage control for major infrastructure problems, such as the loss of power or water." (Jones, 1998, pg.1)

Capers Jones warns, "There will be unrepaired Year 2000 problems, and it is folly to deny it." (Jones,1998, pg. 3) He recommends six goals for municipal year 2000 contingency planning:

[1] Minimize urban damages from unrepaired year 2000 problems

[2] Minimize risk of infrastructure damage due to power or water failure

[3] Optimize the speed of recovery from unrepaired year 2000 problems

[4] Minimize the risks of litigation against government units

[5] Provide accurate status information to concerned citizens

[6] Coordinate local Y2K status with other governments (Jones, 1998, pg. 2)

Because of the vast interconnectedness of information systems, the failure of one may result in the failure of many in a "domino" or "ripple" effect. Sound risk management practices can help to curtail the problem. (Davis, 1998, pg. 85) Contingency planning, including developing alternative plans, manual work-arounds, and fallback procedures for potentially affected systems is essential. "Public safety officials should plan for non-traditional disruptions, such as extended electrical outages; gas, water, phone outages; transportation disruptions; and supply chain disruptions affecting crucial resources, such as food, raw materials and consumer goods." (Davis, 1998, pg. 86)

Public Attitudes

The Bray Survey was designed to measure emotional factors related to Y2k. Designed by four psychologists, the survey measured the dynamic interaction of four factors: knowledge, discouragement, apprehension and denial. Respondents were asked to rate their level of each of the four. The survey indicated positive results as compared to an earlier version. It indicated that between July 1997 and January 1998 there was (1) An increase in Y2K knowledge; (2) An increase in discouragement; (3) As increase in apprehension, and, (4) A decrease in denial regarding the Y2K issue. These results were interpreted to mean that the level of motivation to overcome the problem is growing among the American public. The fact that apprehension was growing was thought to be a hedge against the rise in the discouragement factor. (Nemeth, Creveling, Hearn, & Lambros, 1998, pg. 1

A CNN "quickvote" [sic] results published April 2, 1999, indicated that Y2k ranked 4th among factors listed as concerns to the public. To the question, "Which of these issues causes you the most concern, as we approach the new millennium?", respondents indicated they are most concerned about the growing world population, followed in order by terrorism and nuclear proliferation. Y2K was only of more concern to the 8440 respondents than global warming. (CNN, 1999, pg. 1)

Fifty-one percent of adults 18 years old and older expect minor problems over the Y2K holiday. Thirty-four percent of the respondents expect to experience major problems, while ten percent expect no

problems at all. These results were from a *USA Today/Gallup* telephone poll conducted between December 9-13, 1998. Although 40% reported to be somewhat concerned (and 16% very concerned), respondents indicated that they did not expect problems to impact them personally very much. Seventy-nine percent expect problems to last more than several weeks, and up to more than one year. When asked about stockpiling food, water or taking money out of the bank, well over half of the respondents indicated that they had no plans to make such preparations. The poll showed that 1,032 American respondents trust government at all levels to have the problem fixed before the deadline arrives, but are not confident that the rest of the world will be prepared. (USA Today/Gallup, 1998, pg. 1-6)

Summary

It is evident from the literature that, although the United States has made great strides in correcting Y2K in the past year, it is still probable that there will be serious infrastructure and economic problems. It is equally clear that the responsible action to take for public officials is to require complete contingency and service continuity plans to be ready as soon as they can be practically written. The attitudes of Americans indicate that preparation by governments at all levels is a basic expectation. In fact, polls indicate that most Americans will leave all of the preparation to government. In order to fulfill the public trust, emergency services departments must make plans and provisions for the possible, the unlikely, and the unthinkable.

PROCEDURES

Preparing the Plan

A series of fortuitous circumstances directed the researcher toward the particular project undertaken. First, in January 1998 the researcher took the National Fire Academy's Executive Analysis of Fire Service Operations in Emergency Management course in anticipation of applying for the Executive Fire Officer's Program (EFOP) and, upon acceptance, counting it as the program elective. In the late summer

of 1998 he heard a taped presentation of potential Y2K problems which piqued his interest. This event was followed shortly by notification of conditional acceptance into the EFOP. As the researcher contemplated a topic for study he became aware of the City of Austin Y2K planning effort, of the near completion of the Technical Compliance portion and the Department's pending need to research and write a Service Continuation Plan. The researcher requested permission to have the responsibility of the project. Fire Chief Gary Warren agreed, and the project was assigned to the researcher.

The first action was a literature review in early November at the NFA's Learning Resource Center. Fifteen fire service publication references were found, all published since mid-1998. In the weeks following, the researcher conducted various Internet searches for literature and found more material than could be assimilated.

Though finding material was not a problem, sorting and wading through the literature was difficult. After a while it seemed that most of the literature contained largely the same body of knowledge rearranged in a different order. The researcher examined the attitude extremes, and all of the perspectives in between. Material from many infrastructure industries and services was examined: electrical, water and wastewater, transportation, communications, information services, the natural gas and oil industry, health care, and government services. It was vital to periodically and regularly review the print and electronic media because Y2K preparation conditions are changing rapidly.

In January 1999 the researcher began participating on the City of Austin's "Austin 2000" taskforce, assembled from all departments within the City to prepare for Y2K. The series of meetings was designed for information sharing between departments and presenting information helpful in the writing of each department's SCP. The City Of Austin Information Services Office personnel chaired the meetings. The semi-monthly meetings presented updates from departments of common interest to others, such as Information Services, 9-1-1 Center, Austin Energy, Water and Wastewater, and Fleet Services. Information from these was factored into the AFD's SCP as it was written.

Overall project responsibility for the AFD SCP was assigned to AFD Division Chief Phil Jack. The researcher was assigned to research and assimilate available information; participate in planning meetings; write the draft document; submit the draft to the AFD Command Staff; participate in their discussions and answer questions; then put it in finale form for adoption following Command Staff input.

The researcher also worked closely with Steve Collier, City Of Austin Emergency Manager, and Lindy McGinnis, Emergency Planner for the Officer of Emergency Management (OEM). They provided information on standardized format for the AFD SCP in order to merge into the overall City plan. Also, the AFD takes a lead role in the staffing and processes conducted in the EOC when activated, so it was important that the Department's plan dovetail into the OEM's plan.

The OEM published a template for the City of Austin plan document. The template provided an important framework for organizing the plan material. The researcher also gathered and considered example plan templates from the following agencies/organizations during its writing:

University of Minnesota	U.S. Nuclear Regulatory Commission	Austin Energy
City of Austin Fleet Services	Montgomery County, MD	Department of the Navy
State of Minnesota	State of Connecticut	State of Texas
FEMA	City of Hartford, CN	Mesa, AZ Fire Dept.
State of Georgia	City of Plano, TX	City of Victoria, TX
City of Lubbock, TX	City of Austin Water and Wastewater	

The diversity of approach was the striking feature of this information search. Literally, the plans differed by tens to hundreds of pages in length. There were dramatic differences in philosophy and expectation of the seriousness of the Y2K event. There was also a vast difference in the level of detail provided by the different plans.

In the first week of January 1999 the researcher wrote and distributed a survey to the attendees at the Texas Association of Fire Educators (TAFE) Conference. Of the 103 surveys distributed, 66 were returned completed (64%). This group was selected as target survey group because they represented a

large gathering of fire service personnel from within the State of Texas. The researcher felt that it would be valuable to measure the actions taken by those in a similar environment. Also, most of the attendees were not in the executive level of leadership in their respective departments, and it was deemed desirable to measure the "trickle down" of Y2K preparation knowledge in those departments and agencies represented.

On January 13, 1999, a copy of the same survey with cover letter was mailed to the members of the Metro Chiefs' organization of the International Association of Fire Chiefs. In this sample 125 surveys were mailed and 66 responded (52.9%). The total response to both surveys, state and national, was 228 distributed, 131 responses for a response percentage of 57.5%. A copy of the survey with a tabulation sheet can be viewed in Appendix E.

The Metro Chief's Association was chosen for survey because fire departments in cities with population bases of greater than 200,000 have the most in common with the City of Austin (population 665,000+). It was felt that other large departments might well face the same issues Austin currently faces while making hard planning decisions for the event. This sample also gave the researcher an across-the-country outlook of how this problem was being viewed by the industry. The survey was mailed to the addresses listed by department on the latest Metro Chiefs membership list.

The purpose of the survey was to measure the awareness level of large fire departments across the country, and,

1) To gauge the readiness of those departments who are planning for Y2K;
2) To find out how many departments would be relying on their all-purpose disaster plan rather than develop an incident-specific plan;
3) To find out who (if anyone) was preparing a similar plan;
4) To gauge the level of detail being addressed in existing plans; and,
5) To gauge the attitude/expectation of problems as related to call volume for the event.

Prior to the return of the surveys the researcher expected responses to reflect little or no

knowledge of Y2k issues in most departments. The researcher also expected to find the same extremes in attitude in fire service as exist in the general population: ignorance of the issues or complacency versus expectation of catastrophe. Pragmatism is common in the fire service. Also, grave emergencies are not uncommon in the industry, and the fire service generally enjoys successful outcomes. Because of these factors the researcher expected that those fire service managers who had knowledge of Y2K would likely dismiss the event as trivial, or at least well within their capabilities to cope. The researcher expected to find few example plans to be in existence or even in development.

In the cover letter to this survey, the researcher chose to define the following terms for clarity:

Y2K Mitigation Plan—Actions planned or taken (other than normal operating procedures) to prevent or lessen the impact of the loss of computers or computerized functions. Examples include updating programming, reprogramming, replacing older equipment, date rollover testing, etc.

Y2K Service Continuity Plan-- Actions planned or taken (other than normal operating procedures) to ensure the necessary logistical or staffing support for uninterrupted emergency services to citizens. Examples include such activities as providing alternative electrical power, storing food or drinking water, storing extra fuel, arranging for extra staffing or reserve units to be placed in service, etc. (Templeton, 1999, pg.1)

The expectation of problems as related to call volume was an important aspect of this survey, made more so by the fact that experts in the Information Technology are unable to predict with clarity the outcome of the date rollover. Overwhelmingly, fire service managers reported that they believe Y2K will present only minor problems, with few increases in call volume (see page 36, "Results").

As the researcher was writing the final drafts of this paper, the *Contingency and Consequence Management Planning for the Year 2000 Conversion* guide arrived. This booklet confirmed the federal government's position that emergency services providers should be actively planning for temporary disruptions. It is a very informative guide for emergency services departments for developing a

contingency plan (Service Continuity Plan). It was distributed through the Training Resources and Data Exchange (TRADE) program, and the researcher examined the booklet for concepts that had not been encountered from other sources.

Limitations

The researcher experienced three major limitations regarding the nature of the research problem, and three personal limitations. The principal limiting factor for this research project was the ambiguity of expected outcomes for the Y2K date rollover. Because no one knows or can predict with assurance what failures will occur, this project had to prepare for what may occur—a higher standard to meet.

The second limitation is related to the first, but differs slightly. The vastly divergent published viewpoints, each seemingly sure of their position, made the formation of planning assumptions difficult. The researcher, having little expertise in Information Technology, was placed in a position of making an "educated guess" when evaluating the literature. As explained earlier, psychological factors tend to keep most individuals in the middle-of-the-road when it comes to Y2K, even if there is credible evidence to the contrary.

A third major limitation was the changing nature of the problem during the research period. In the six months between October 1998 and April 1999 the problem changed dramatically as progress was reported and improvement was achieved in both the private sector and in government. Many factors that had been established and credible earlier were found no longer to be relevant toward the end of the research window. This fact leads the researcher to believe that similar progress may be made in the remaining months, reducing the domestic impact of Y2K from what was originally thought, and moderating preparation actions.

The first personal limitation for the researcher was the difficulty of working within a team yet writing the plan individually. This proved to be a minor inconvenience associated mostly with scheduling and approval of plans by higher authority.

The second personal limitation was more difficult. The researcher was working under an EFO-required six-month deadline (April 14, 1999) which was in conflict with the City of Austin internal deadline of May 14, 1999. It became apparent that the SCP would be changing regularly as new information was processed until turned in to the Office of Emergency Management on May 14. Wishing to complete the final plan prior to sending in the research project to the NFA, the researcher sought and received permission for a one-month extension. The extension resolved the conflict, as the researcher would now be able to include a final product with the research paper.

Finally, the researcher entered this project (his first EFO applied research project) without the benefit of the NFA's Executive Development course. In retrospect, not having the course has resulted in increased difficulty in discerning the paper requirements and mapping the most beneficial process.

RESULTS

Answers to Research Questions

The researcher proposed the following questions as important information affecting the final development of a Y2K Service Continuity Plan for the AFD. The answer for Research Question #1 was gleaned from the literature review and the Austin 2000 project. A survey instrument was used to measure final results for Questions 2-4.

Research Question #1: What is the likelihood of the occurrence of significant infrastructure problems associated with Y2K?

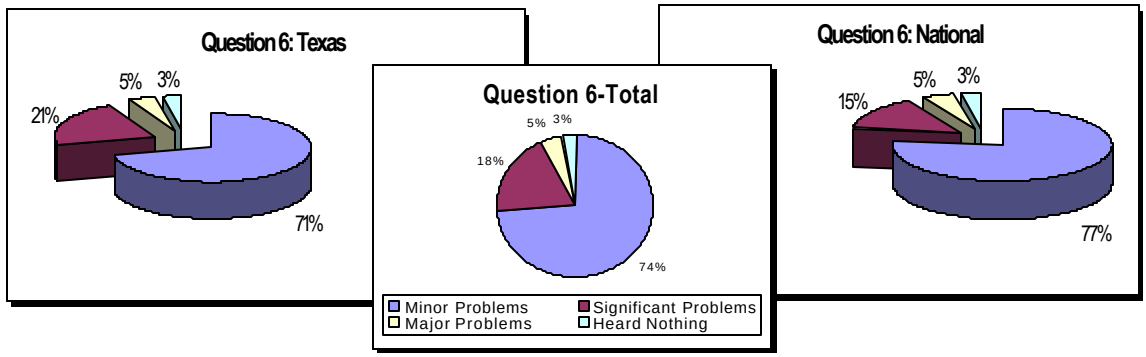
The researcher found no known measurable scientific data to support a definitive conclusion. The absence of such data seems to be the major difficulty in predicting the seriousness of the event, and is the reason for the most common conclusion drawn by writers on this subject: nobody knows! Even with the program testing records of government and corporations, enough variables remain to blur the true picture.

However, there was available an abundance of anecdotal information. The researcher concluded that this question could only be answered subjectively based on conclusions drawn from reading after various sources, and after weighing their reputation for reliability and considering their expertise.

A conclusion was drawn that some degree of infrastructural malfunction is likely (better than 50% likelihood). However, these malfunctions are most likely to be spotty or regional in scope, short-to-moderate in duration, but may well result in heavy increases in emergency call volume for the critical period of December 31, 1999, through January 5, 2000. Infrastructural malfunctions are likely to continue through mid-year, and taper off toward the end of year 2000. Small to medium-sized cities and companies seem to be more vulnerable due to their lack of preparedness at this point, and may be the focal point of many of the infrastructure malfunctions. One reason for this fact is that they have enough technology to cause problems, but lack the ability to make major funds commitment required to remediate their equipment.

Research Question #2: What are the expectations of others in the fire service community concerning Y2K problem significance and call volume?

Figure 1



<u>Question #6</u>: Considering what you have heard or read about Y2K computer problems, which of the following describes your current expectations?

Metro Chiefs' Survey Results

50) I expect minor problems with few increases in emergency call volume.
10) I expect significant problems with moderate increases in emergency call volume.
3) I expect major problems with dramatic increases in emergency call volume.
2) I have heard little or nothing about Y2K

(Figure 1 cont'd from page 36)

Texas Association of Fire Educators' Conference Survey Results

47) I expect minor problems with few increases in emergency call volume.
14) I expect significant problems with moderate increases in emergency call volume.
3) I expect major problems with dramatic increases in emergency call volume.
2) I have heard little or nothing about Y2K

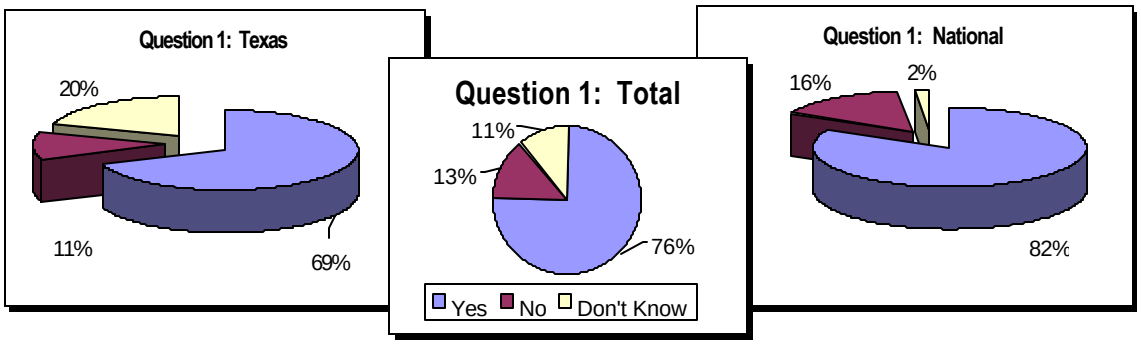
Survey Question 6 was designed to measure fire fighter's attitude and expectations about the amount of disruption caused by Y2K, and any subsequent anticipated increase in workload. Figure 1 reveals that the results from both the in-state surveys and the Metro Chiefs' surveys are remarkably similar with regard to Y2K expectations. Both surveys were conducted at a time before the recently published information about progress in meeting programming goals. In other words, well before there was reason for optimism, fire fighters discounted the possibility of a serious situation.

The surveys received 65 and 66 responses, respectively, to this question. Seventy-seven percent (77%) of Metro Chiefs expect only minor problems, while seventy-one percent (71%) of fire service instructors expect the same with few increases in call volume. Though small, the disparity can perhaps be explained by the fact that Metro Chiefs are in a position to influence Y2K preparedness, and therefore may be more confident in the outcome. The potential danger of this level of confidence may be the tendency not to prepare fully for that which one does not consider likely. Significant problems were expected by 15.4% of the chiefs, and 21.2 per cent of the educators. Only 4.5% of both groups expect major problems.

The researcher compared these results to the *USA Today/Gallup* poll conducted December 9-13, 1998. The poll interviewed a random sample of Americans by telephone. Of the 1,032 persons interviewed, only 51% expect minor problems, 34% expect major problems and 10% no problems at all. (USA Today/Gallup Poll, 1998, pg. 1) Based on the juxtaposition of these three surveys, it appears that fire service personnel are considerably more optimistic (approximately 50%) about the degree of seriousness of Y2K than is the general public.

Research Question #3: Are other fire departments developing mitigation strategies and service continuation plans? If so, are these usable as a planning model for AFD?

Figure 2



Question #1: Does your department have a Disaster Recovery Plan generic to any emergency situation?

Metro Chiefs' Survey Results

51--Yes (82.5%) * 15--No (15.9%) 1--Don't Know (1.6%)

Texas Association of Fire Educators' Conference Survey Results

45—Yes (69.2%) * 7—No (10.9%) 13--Don't Know (20%)

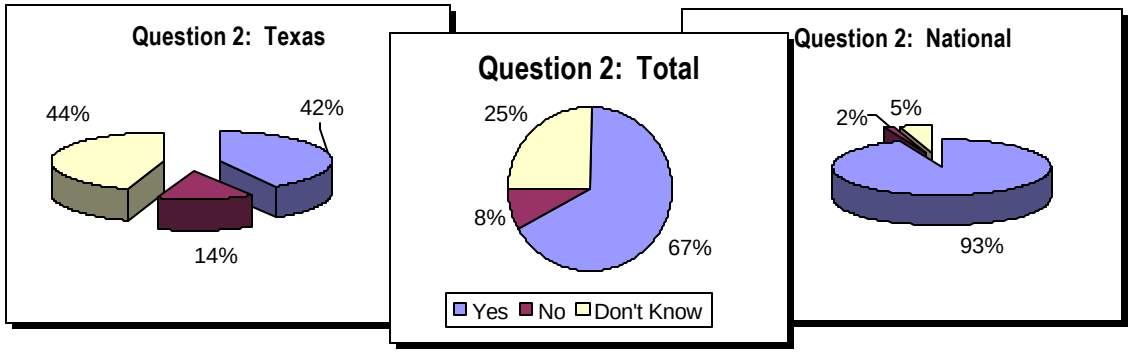
*** A list of cities answering "yes" may be found in Appendix E.**

Research Question #3 was answered by Survey Questions #1, #2, and #3. Survey Question #1 shows that most emergency services departments have disaster plans in place. The merit of this question was as a comparison factor between this and questions two and three dealing with Y2K planning. The goal was to correlate any existing relationship between Y2K and other disaster planning (see discussion following Figure 4). If the city does not have an all-purpose disaster plan, but does have a Y2K service continuity or recovery plan, it could be inferred that the city considers the threat more credible and eminent than, for example, a tornado, flood or hurricane. If the city has a disaster plan with no Y2K plan, the indication is that the threat of Y2K does not rise to the level of threat presented by other disaster types for those cities (attitudinally speaking).

Survey Question #1 responses show that a greater percentage of metro cities have disaster plans. One possible explanation is that since many large cities are required through SARA Title III to participate in Local Emergency Planning Committees, they must have hazmat disaster plans. Many states also require plans for other disaster types for large jurisdictions.

The number of "Don't Know" answers was significantly higher for the TAFE Conference survey (20%) than for the Metro Chiefs' survey (1.6%). The most reasonable explanation for this fact may be that the conference attendees are generally lower ranking members in their respective organizations than the target audience for the Metro Chiefs' survey. Personnel lower in an organization's rank structure tend not to be as familiar with information on the order of citywide disaster plans. If true the lack of communication concerning the plans calls into question their workability when they are needed. One surprising result of this question was that more than twice as many metro city respondents reported not having a disaster plan compared to the TAFE conference participants.

Figure 3



<u>Question #2</u>: Does your city have a Y2K Mitigation Plan?

Metro Chiefs' Survey Results

59—Yes (93.7%) * 1—No (1.6%) 3--Don't Know (4.7%)

Texas Association of Fire Educators' Conference Survey

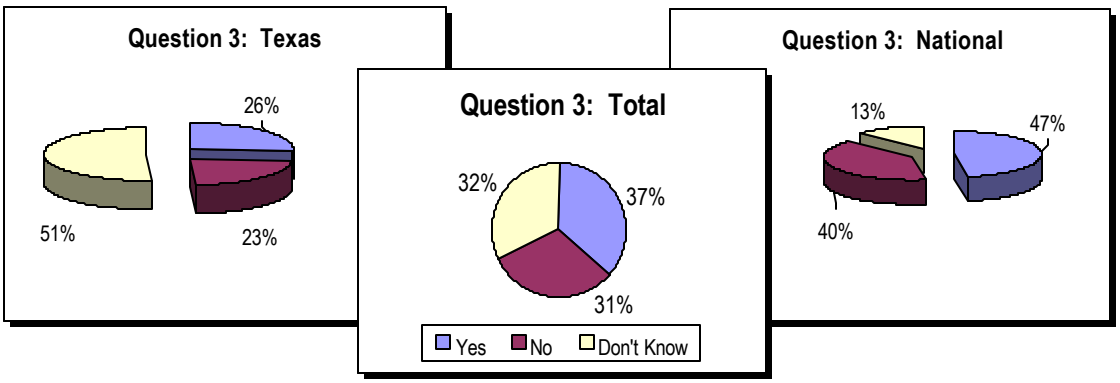
27—Yes (26.2%) * 9—No (13.8%) 29--Don't Know (44.7%)

*** A list of cities answering "yes" may be found in Appendix E.**

A Mitigation Plan was defined for the purposes of this survey as "actions planned or taken (other than normal operating procedures) to prevent or lessen the impact of the loss of computers or computerized functions." Overwhelmingly, metro cities have recognized the need to mitigate their computer systems' Y2K problems. It is surprising, however, that at least one major city has not yet begun remediation work, and three other respondents are not aware of a plan if it exists. This result is surprising because, considering the complexity of the task for most municipalities, time is running short for those who have not yet begun.

The same possible explanation applies to the TAFE's "Don't Know" answers as with Survey Question #1. It does not appear that communication concerning the Y2K problem has been cascaded to lower ranks.

Figure 4



<u>Question #3</u>: Does your department have a Service Continuation Plan specific to Y2K?

Metro Chiefs' Survey Results

30—Yes (47%) 25—No (40%) 8--Don't Know (13%)

<u>Cities who answered *Yes*:</u>

Aloha, OR	Columbia, MD	St. Paul, MN	Honolulu, HA
Philadelphia, PA	Hartford, CT	Des Moines, IA	Bakersfield, CA
Aurora, CO	San Diego, CA	Richmond, VA	Phoenix, AZ
Tacoma, WA	Kansas City, MO	Milwaukee, WI	Memphis, TN
Ft. Lauderdale, FL	Winter Park, FL	Tucson, AZ	Worchester, MA
Los Gatos, CA	Arlington, TX	Garland, TX	Plano, TX
Mesa, AZ	Ft. Worth, TX	Atlanta, GA	Houston, TX
Albuquerque, NM	Los Angeles, CA		

(Figure 4 cont'd next page)

(Figure 4 cont'd)

Texas Association of Fire Educators' Conference Survey Results

17—Yes (26%)		15—No (23%)	33--Don't Know (51%)
Cities who answered Yes:			
Allen	Groves	San Angelo	Euless
Irving	Sherman	Flower Mound	Kellar
Sugarland	Garland	Kingsville	Texarkana
Grapevine	Lubbock	Victoria	

Questions 1, 2 and 3 were designed to measure individual fire departments' attitude toward disaster planning in general, and then specifically concerning the Y2K problem. By doing so it was hoped that a pattern would emerge that would further indicate the fire service attitude concerning the Y2K, and how it rated in seriousness compared with other types of disaster.

The answer to Research Question #3 is that many departments are aware of the need for remediation, and have addressed the problem through a mitigation process (67%). Larger cities seem to have a better appreciation for the need to plan for disasters in general, and Y2K specifically. One reason for this could be a greater reliance on technology in critical processes. Y2K SCP's overall do not appear to the rule, but the exception, with only 37% answering affirmatively that a plan is in place or in development. However, the large majority of the plans that do exist are still in process and are therefore not suitable as a model for AFD at this time.

Comparing all-risk disaster planning in place to Y2K plans in place, 82.5% of metro cities and 69.2% of TAFE respondents have all purpose plans, but only 47% and 40% respectively have Y2K-specific plans. These statistics may indicate that Y2K is generally not perceived as a threat to the fire service.

On the other hand, 93.7% of metro cities have an on-going Mitigation Plan. The presence of a Mitigation Plan (93.7%), coupled with the lack of a SCP (47%) may indicate, not the lack of respect for Y2K as a potential disaster, but rather a high level of confidence in the success of the remediation efforts.

In a follow up to the metro and TAFE surveys, departments indicating that a SCP was in place

were called by telephone and asked for a copy for comparison. No departments sent copies of a plan when returning the questionnaire, and no plans were received as a result of the phone calls. The departments contacted indicated that the plans were still being developed and would be shared as they are completed.

Research Question #4: What are the likely problems associated with any expected infrastructure collapse, and how can they be prepared for?

Figure 5A

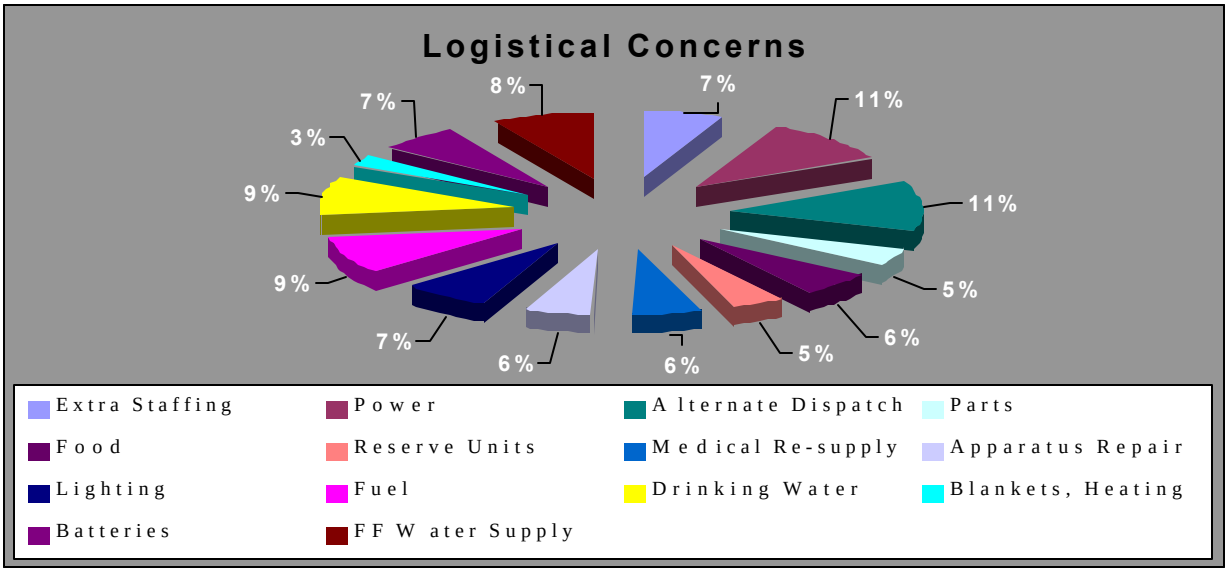
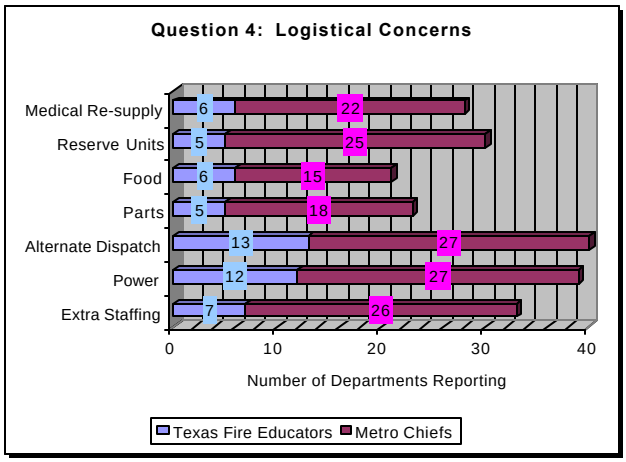
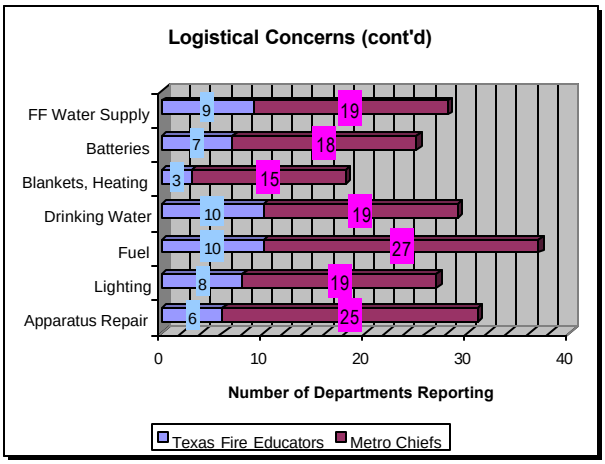


Figure 5B





Survey Question 4 relates to Research Question 4. The survey question listed 14 categories and asked those cities reporting that they have a Y2K plan which categories of logistical items it covered. The survey also provided an "Other" category for additional items that may have been omitted. Figure 5A shows the relationship of each category to the others as a percentage of the whole response. The most common logistical preparations that are being made as part of SCPs are power, alternative dispatch procedures, drinking water storage, fuel, and fire fighting emergency water supply. Departments are apparently least concerned about storing food, blankets or alternative methods of heating, and apparatus parts availability. However, all of the logistical concerns listed received some response. No appropriate "Other" items were listed on survey responses, suggesting perhaps that the list presented is fairly complete. There were, in fact, included on some surveys unsolicited comments that the list appeared complete.

Figure 5B shows the relationship between the TAFE conference and Metro Chiefs' responses in each category. The bar chart shows what percentage of the whole response in each category was from each survey group. Clearly, most of the logistical preparation that is being done for Y2K is by metro cities.

The Austin Fire Department Service Continuity Plan

The final product of this research project was a formal Service Continuity Plan for use by the AFD during the Y2K event. The survey instrument was used to gauge from the industry a sense of the proportion of the emergency expected. It was also used to gauge the degree of detail included in other agencies' plans. A copy of SCP's from those departments responding that such had been prepared was sought, however none had been completed and sent as of this writing. Most departments contacted responded that their plan was also in development and would be shared upon completion. The final AFD plan does take into account information gleaned from other organizations' SCP plan template acquired through the Internet. Attitudes and expectations of other departments helped to shape the formation of AFD's planning assumptions, and therefore influenced AFD's final plan outcome.

The following is an outline for the general topics covered by the AFD SCP. The template for the

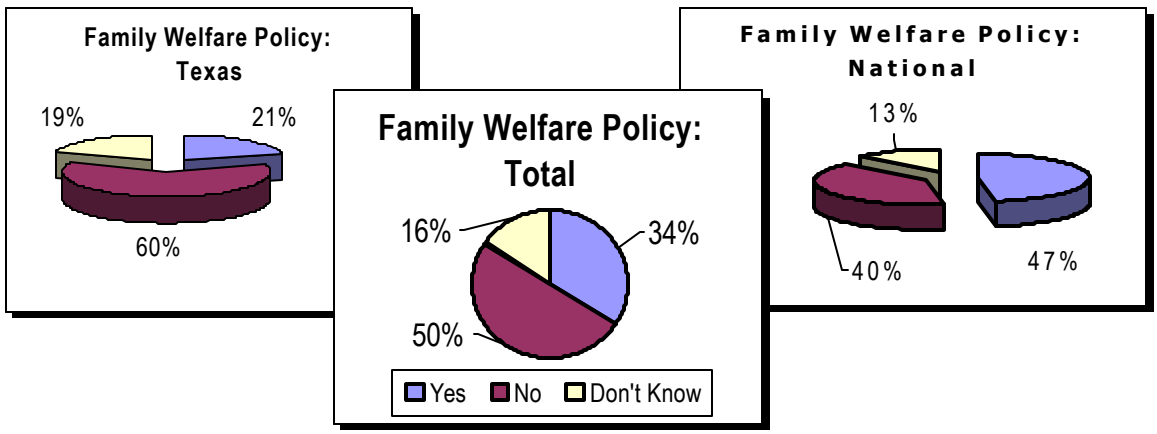
plan was a standard template used by all City of Austin departments, and was developed by the City of Austin Office of Emergency Management. Each of these topics are developed in detail and specific for the AFD. The complete Plan is contained in Appendix A.

- Introduction
  - Purpose of the Plan
  - Executive Summary
  - Scope and Applicability
  - Relationship to Other Plans
- Situation and Planning Assumptions
  - Anticipated Situation or Conditions
  - City of Austin Planning Assumptions
  - Departmental Planning Assumptions
- Mission and Critical Services
  - Mission of the Austin Fire Department
  - Prioritize Critical Services
  - System Priorities
  - Customer Priorities
  - Service request Priorities
- Plan Execution
  - Plan Activation
  - Crisis Management Organization
  - Situation Assessment
  - Increased Service Demand
  - Requesting Outside Resources

- Post Incident Recovery
  - Returning to Normal
  - Post Incident Review Process
- Administrative and Logistical Support
  - Staff and Materials Required
  - Human Resource Policies and Procedures
  - Special Procurement Procedures
  - Family Support and Crisis Service
  - Facilities

Emergency Family Contact Policy

Figure 6



Question #5: Does your department have a policy and procedure for keeping on-duty emergency workers in touch with family members during times of crisis?

Metro Chiefs' Survey Response

27—Yes (34%) *	32—No (34%)	4--Don't Know (16%)

Texas Fire Educatorss Survey Results

13—Yes (47%) *	38—No (40%)	12—Don't Know (13%)

* A list of cities answering "yes" may be found in Appendix E.

A critical piece of any all-hazards disaster policy is a plan to put emergency workers in touch with immediate family members to ensure their safety. Without assurance that one's family is out of harm's way, there is a real possibility that fire fighters will not stay at work. The AFD does not currently have such a policy. As an adjunct project to the SCP, Survey Question #5 was included to gather information for implementing a Family Welfare Policy. AFD will be requesting information on other departments who indicated in response to Survey Question #5 that they currently have such a plan in place. The survey indicated that 96 departments have an all-hazards disaster recovery plan, yet only 40 have a Family Welfare Policy. The AFD will attempt to have a policy in place before December 31, 1999.

DISCUSSION

Literature Review and Survey Results Compared

The researcher expected the results of the Y2K Surveys to show that there was widespread ignorance of issues or complacency toward the Y2K problem within the fire service. Though it showed that many metropolitan department have not given this matter appropriate attention, more than expected had begun service continuity planning, and knowledge about the issues involved appears to be steadily growing. When contacted to share a copy of their plan, it became evident that the fire service is not ready for Y2K, but is rushing to get ready. Not a single department that had checked "yes" in answer to Survey Question #3 sent a copy of the plan with the return as requested by the survey. When a follow up phone call was made to request a copy in March 1999, no department had a complete plan to share.

Since the request in March, the researcher has received the completed Y2K SCPs from two cities. Though well written and very readable, in the judgment of the researcher, neither showed the attention to logistical detail that would be important in an urgent situation. The concept used in the AFD SCP was to address as many staffing, logistical support and organizational adjustments as could be anticipated

beforehand in order to provide an opportunity to brief personnel in advance and relieve some stress on command officers during the actual event.

The Literature Review clearly indicated the potential for a serious, even devastating situation with the New Year. Federal government spokespersons have publicly expressed concern for preparation efforts. (CNN, 1999, pg.1) Officials from the President's Council on Year 2000 Conversion have listed among their key priorities business continuity and contingency plans as "…insurance against Federal service delivery and operations from Y2K–related failures." (Koshinen and DeSeve,1999, pp. 1-2) They further urged continued outreach to the public and private sector to encourage contingency planning. (Koshinen and DeSeve,1999, pp. 1-2)

Freeman and Campbell have both written about the need for planning for failure. (Freeman, 1998, pg. 24; Campbell, 1998, pg. 25) Porlier reminds that the final effect of the Y2K crisis is largely dependent of what actions are taken in the interim, both mitigation and contingency, on a local basis. (Porlier, 1998, pg. 20) Experts recognize that when business and industry fails to plan, the results can be devastating; however, when governments--society's safety net--fail to plan, the devastation can be multiplied many times. And, it is generally agreed that the task of contingency planning for governments is more complex that for the private sector, making beginning the task even more urgent. (Jones, 1998, pg. 1) Public safety officials must plan for non-traditional disruptions, and even for a ripple or domino effect of simultaneous loss of multiple infrastructure components. (Davis, 1998 pg. 86) The Y2K Survey indicated that a high number—over three out of four departments—have an all-purpose disaster plan in place. All-hazards plans provide a good base for Y2K planning, but the need for specific and detailed planning is still evident. Once written, these plans have value, not only for the Y2K event, but also as insurance against other types of infrastructure disasters. They also provide a measure of safety against tort liability and future lawsuits alleging negligent failure to plan on the part of the local government.

The Y2K survey response indicates that the fire service needs to turn appropriate attention to the problem of service continuity planning. The total response to the survey indicates alarmingly that just over one in three departments is known to have a SCP in process or completed. Even making allowances for the fact that the TAFE's personnel may not have been highly enough placed in their organizations to be aware of planning efforts, the Metro Chiefs' survey showed less than half of them are planning for service continuity. The U.S. conference of Mayors report that cities on the whole are not doing much better with continuity planning than the fire service, with only 54% reporting that they have a plan. (U.S. Conference of Mayors, 1999, pg. 1)

The final question (unnumbered) of the survey asked if the responding agency wished to have a copy of the results. It is interesting that in response to this question, only three requests for results were received from the Metro Chiefs' survey. The alarming implications may be that whatever level of effort exists, or doesn't exist with regard to the Y2K challenge, respondents appear content with their current efforts, or at least are not interested in learning from the efforts of others. The TFE respondents showed considerably more interest, with 34 requesting a summary of results.

Implications for AFD

The results of the Y2K Survey indicate that the Austin Fire Department may be among the first emergency services departments to have a complete (though living and changeable) Y2K Service Continuity Plan. This fact means that there is not a lot of guidance available from the experience of others to draw upon. Therefore it was incumbent upon the researcher to find other sources for business continuation principles and adapt and apply them to the situation at hand. Other sources were found and developed consistent with theories, principles, and procedures contained within the EFOP curriculum.

Recommendations

Experts in the fields of Information Technology, Community Planning and Risk Management all agree that the most prudent course of action is for organizations to develop detailed Service Continuity Plans. The results of this study have reinforced the Austin Fire Department's planning initiative, and provided guidance in the areas that must be included in the final Plan document.

The problem before the AFD was to, using appropriate and standard research procedures, develop an appropriate SCP to meet the challenge of Y2K. This problem and research purpose have been fulfilled.

The researcher recommends that industry-wide efforts begin to be made to alert emergency services departments to the need for service continuity planning. Major organizations within the fire service should immediately begin to educate their members to the potential problems, and encourage them to be prepared in the event mitigation efforts fall short.

Following adoption of its SCP, the Austin Fire Department should now shift its focus to completion of supplemental policies, and to publication and education of AFD employees concerning the Plan requirements. (The TAFE survey indicated a high degree of lack of information at lower levels of the surveyed departments. For any plan to be effective, its requirements must be common knowledge throughout the organization.) The Department should schedule an exercise to practice and test the Plan. The Department should continue to carry out its parallel effort in remediation of problems. New supplemental equipment required by the SCP must be designed, specifications written, purchased, and fire fighters given the opportunity to become familiar with it. Public education initiatives should be undertaken to assure citizens that emergency services providers are making preparations to ensure their continued safety. Finally, the Department should continue to scan the environment for changes in the Y2K preparedness status of both the public and private sectors.

REFERENCES

Cable News Network Interactive. White House, nearly half of federal agencies miss Y2K deadline, (March 31, 1999), http://cnn.com/TECH/computing/9903/31/federal.y2k/, pp.1-3.

Cable News Network Interactive. Senate report says Y2K would not pose major disruptions [sic], (March 2, 1999), http://www.cnn.com/ALLPOLITICS/STORIES/1999/03/02/senate.y2k/, pp. 1-5.

Cable News Network. quickvote [sic], (April 2, 1999), CNN Interactive, http://www.cnn.com/POLL/results/119701.html, pp. 1-2.

Cairncross, Francis (Ed.). Survey, the Millennium Bug: From our readers, The Economist Newspaper, (9/19/98), http://economist.com./editorial/freeforall/19-9-98/bug10.html, pp. 1-17.

Campbell, Robert P. Year 2000: Planning to Fail, Contingency Planning and Management, (July/August 1998), Vol. 3, No. 7, pg 25.

Cutter Consortium, Summit '98, (1998), http://www.cutter.com/summit/eyslides/sld005.htm, pg.1.

Christiansen, John. Gearing up for the gold rush [sic], (March 23, 1999), CNN Interactive, http://cnn.com//TECH/specials/y2k/stories/y2k.goldrush/, pp. 1-4.

Davis, Steve. Don't Get Caught With Your Computer Down, Public Risk Magazine, (May/June 1998), Vol. 12, No. 5, pp. 85-86.

De Jager, Peter. Testimony to the House of Representatives Science Committee: Unjustified Optimism, (May 14, 1996), http:/www.year2000.com/archive/testimony.html, pp. 1-3.

Diederich, Tom. Important U.S. computer systems likely to miss Y2K deadline [sic], CNN Interactive, http://cnn.com/TECH/computing/9903/31/behind.y2k.idg/, pp. 1-3.

Entous, Adam. Y2K May Spark Civil Unrest, Economic Pain—US Senate, (1999), Excite News, a product of Reuters News Agency.

FEMA/USFA/NFA-EAFSOEM-SM, Executive Analysis of Fire Service Operations in Emergency

Management Student Manual, (July 1997), pp. SM4-6.

Freeman, LeLand G. Time's Up!, Contingency Planning and Management, (July/August 1998), Vol. 3, No. 7, pg. 24.

Gershwin, Lawrence K. Testimony of Lawrence K. Gershwin, National Intelligence Officer for Science and Technology, National Intellegence Council, Government Management, Information and Technology Subcommittee of the House Government Reform and Oversight Committee, (January 20, 1999), http://www.y2k.gov/new/hornY2K2.htm, pp. 1-3.

Graham, Allan. The Year 2000: Test or Be Tested. Contingency Planning and Management, (July/August 1998), Vol. 3, No. 7, pg.26.

Jones, Capers. Report: Year 2000 Contingency Planning for Municipal Governments, (August 15, 1998), http://www.angelfire.com/mn/inforest/capersj989.html, pp. 1-11.

Koshinen, John A., DeSeve, G.Edward. Press Release: FEDERAL GOVERNMENT NEARS COMPLETION OF Y2K WORK ON MISSION-CRITICAL SYSTEMS [sic], (March 31, 1999), President's Council on Year 2000 Conversion, http://www.y2k.gov/new/0331PRL2.htm, pp. 1-2.

Larson, Randall D. Facing the Year 2000: Is your PSAP prepared for the Century Mark? (May/June 1998), 9-1-1 Magazine, pp.42-44, 45.

McCracken, Judith. Quality Through the Lens of System Thinking, (1995), Thoughtspace, Inc., pg. 6.

Missler, Chuck. The Millennium Bomb: Y2K, (1998) Tape Series, Koinonia House, Coerd'Alene, ID.

National Association of Counties. Press Release: Half of the nation's counties have Y2K strategic plan, $1.7 billion needed to reach Y2K compliance [sic], (December 8, 1998), http://www.naco.org/pubs/releases/y2ks.cfm, pp.1-2.

Nemeth, Darlyne, Ph.D., Creveling, C. Christiane, M.A., Hearn, George E., Ph.D., & Lambros, John D., B.S. (1998), The Bray Y2K Survey: Positive Trends in Survey Data,

http://www.year2000.com/archive/bray.html, pp. 1-5.

Pierce, Ellise. Millennium Bug Smasher. American Way Magazine, Nov. 1, 1998, Vol. 31, No. 21, Pages 86-92.

Porlier, Victor. Y2K: Get your Action Plan in Order Now, Public Management Magazine, (October, 1998), pp. 17-21.

Regan, Mary Beth. Countdown to a Crash: Billions spent, yet computer disruptions still likely [sic], Austin American Statesman, (Jan. 3, 1999), Vol. 128, No. 161, pp. 1, 19.

Sells, Peter. What if the Panic Button Isn't Plugged In? The Fire Services Journal, (Sept/Oct 1998), Vol. 1, No. 6, pp. 16, 19.

The Economist Newspaper. Are You Ready?, (1998), http://www.economist.com/editorial/freeforall/19-9-98/bug4.html, pp.1-4.

The Economist. Survey: The Millennium Bug: Small Cause, (9/19/98), http://www.economist.com/editorial/freeforall/19-9-98/bug2.html, pp. 1-3.

Wierzbicki, Barbara (Ed.). The Year 2000 Problem, The Sentinel, (First Quarter 1998), Vol. LV, No. 1, pp. 3-14.

Templeton, Douglas R. Y2k Service Continuation Survey, (January 13, 1999), See Appendix E, pp. 1-2.

Thorpe, Fred. Y2K Time Bomb—The Crucial Readiness Challenge, Responder Magazine, (May 1998), Vol. 5, No. 5, pp. 8-10.

Thorpe, Fred. Y2k Bomb—The Crucial Readiness Challenge, Part II, (June1998), Responder Magazine, Vol. 5, No. 6, pp.6, 8, 30.

Thorpe, Fred, and Bramblette, Denis. Waking Up to Y2k, (July 1998) Responder Magazine, Vol. 5, No. 7, pp. 6-7.

U.S. Conference of Mayors. Press Release: The Status of Y2K Compliance in City Governments,

(January, 1999), http://208.210.12.207/uscm/y2k/y2kfindings.html, pp. 1-33.

USA Today/Gallup Poll. AMERICANS AND THE Y2K MILLENNIUM COMPUTER BUG [sic], (December 1998), http://www.y2k.gov.new.y2ktopline.html, pp. 1-9.

Verton, Daniel. Y2K failures abroad threaten U.S. security [sic], (March 1, 1999), CNN Interactive, http://www.cnn.com/TECH/computing/9903/01/y2ksecurity.idg/, pp. 1-3.