

The Impact of the Y2K Threat on Hospital Emergency Preparedness

Rory Connell

Disaster Research Center, University of Delaware

Research Supervisor: Kathleen Tierney, Director

Summary

The Y2K threat provides an excellent case study of organizational perception of and adjustment to risks. Utilizing qualitative data collected from focus group interviews with thirteen health care organizations, this paper examines hospital risk perception and preparedness for the Y2K computer problem. The potential for a date-specific failure of technological systems required hospitals to identify shortcomings of their emergency preparedness by significantly reassessing contingency plans, critical-care technology, and emergency supplies. The Y2K threat required a multi-departmental focus on emergency preparedness. In addition, many hospitals indicated that emergency plans were coordinated with external organizations, such as other hospitals and vendors. The paper concludes by suggesting implications of the Y2K case study for earthquake and natural hazard preparedness in hospitals. The manner in which hospitals responded to the Y2K problem suggests the potential for these organizations to effectively mitigate against perceived risks.

Introduction

While the potential impact of the Y2K problem on computer systems was a focus for many organizations during the late 1990s, the health care industry was particularly concerned about how the millennium bug could affect organizational functionality. Hospitals were vulnerable to the Y2K threat for two primary reasons. First, the majority of the daily functions of hospitals are intrinsically linked to computer systems, from the health-related services that hospitals provide to the basic operations of facilities. Second, because hospitals serve as key elements of a community's infrastructure, their continued functionality during disasters is an essential component to disaster resistant communities. In times of crisis, hospitals must provide medical service to those that were hospitalized before the disaster event as well as those that need medical attention as a result of the event (Alesch and Petak 2002). Quite often, hospitals are expected to function *more efficiently* in these times of crisis due to the heightened level of importance of hospital services in the disaster period (Whitney et al., 2001, Giacometti 1999, Howe 1998).

Although the darkest prophecies of the Y2K doomsayers did not materialize, the Y2K threat does provide an excellent case study of organizational perception of and adjustment to risks. Unlike most disaster events, the Y2K problem represented a *time-specific* and *date-certain* event. Because of the hard deadline for systems compliance to the threat, Y2K focused the attention of both organizations and the media. Y2K was also an unprecedented organizational problem due to the potential for *failures in multiple systems*. The worst-case scenario projections for Y2K warned that a disruption to one system could affect countless other systems. Because of their dependence on public infrastructure systems

as well as organizations such as medical insurer payers, banks, and medical suppliers (Goldberg 1997), hospitals were also vulnerable to the malfunctions in external computer systems. Therefore, from an organizational perspective, Y2K could be considered both an internal and an external risk (Goldberg 1997). Finally, the Y2K threat was not limited to a specific geographic area; therefore, the *scope* of the potential impact was significantly larger than most risk events.

This paper will examine hospital risk perception and preparedness for the Y2K computer problem. The paper utilizes data on hospital mitigation collected by the Disaster Research Center (DRC) at the University of Delaware as part of its research on rehabilitation impediments and incentives. In the interviews, the focus groups were asked to relate recent experiences with hazard events and to discuss the impacts those events had on their preparedness and mitigation decision-making, including their decisions with respect to earthquake hazards.

Based on focus group interviews, this paper will identify common themes in the Y2K experiences of hospitals. The paper has three sections. First, it will provide a description of the study and the methodology utilized in the research, as well as a brief description of the study participants. Second, it will discuss three common themes in Y2K experiences of hospitals: (1) that the Y2K threat significantly influenced hospital preparedness; (2) that, unlike some threats, Y2K preparations required participation from entire organizations; and (3) that hospitals often coordinated their emergency plans with other organizations. Third, it will discuss why health care organizations were more likely to adopt mitigation measures for the Y2K problem than for natural hazard threats.

Methodology

Funding for the research was provided by the Multidisciplinary Center for Earthquake Engineering Research (MCEER). Researchers from the DRC (including the author) visited hospitals in three regions of the United States that faced three different levels of seismic risk (Southern California, which has a high level of risk, Tennessee, which has a moderate risk of seismic activity, and the New York metropolitan area, which has a low level of risk). While the research methodology was constructed around the level of seismic risk, the interview guide that was used for the focus groups was developed to address all of the internal and external risks that these organizations may face.

Hospital Selection

The study sample consisted of a total of thirteen hospitals: four California hospitals, five Tennessee hospitals, and four New York hospitals. Several criteria were used to select the study hospitals. First, the hospitals were required to be acute-care facilities with emergency rooms or trauma centers. Second, hospitals in each region were selected based on the size of the hospital organization, as measured by the number of beds. For the purpose of our study, a hospital with less than 150 beds was considered small, a hospital with 151 to 300 beds was considered medium-sized, and a hospital with 301 or more beds was considered a large facility. Third, hospitals with different types of ownership were selected. Study hospitals included public facilities, proprietary (or private) organizations, and nonproprietary (or not-for-profit) organizations. Fourth, while most of the selected hospitals were in a major metropolitan city in each of the three regions, a hospital in a smaller city in the same county was selected for each of the regions. The non-metropolitan facilities were selected in order to study the impact of city safety and building codes on hospital mitigation, as well as the role that hospital networks and associations in the city may play in risk perception and preparedness.

Focus Group Interviews

Once the hospitals were selected, DRC researchers contacted hospital administration in order to organize focus groups with key decision-makers within the hospitals. The focus group interviews included a diverse group of hospital employees. Typical focus groups included at least one representative from each of the following four groups: hospital administration, physicians, nursing, and engineers.

A total of seventy-six subjects participated in the study, representing a diverse range of professions. Typically, the focus group participants were also active members of their hospital's safety committee. As a result, the majority of the focus group participants had been involved in safety issues and emergency preparedness policies in their hospitals.

Hospital Experiences with the Y2K Problem

The media provided extensive coverage of Y2K preparations in hospitals and endless speculation about the possible outcomes of the event. When the transition into the new year occurred without any major incidents, the media provided little to no follow up on the impact of Y2K preparations on hospitals. Views of the Y2K threat in hospitals quickly shifted from a potentially life-threatening problem to the depiction of the Y2K problem as a media fabrication that was characterized more by hype than risk. While the media focus on Y2K quickly tailed off after January 1, 2000, hospitals were significantly altered as a result of their Y2K preparations. As a consequence of Y2K, hospitals revised their contingency plans, established task forces to combat the Y2K problem, replaced non-compliant technology, and increased emergency supplies.

Based on the focus group data, this section will show how Y2K preparations affected hospitals, focusing on: (1) the impact on hospital preparedness for emergency events; (2) the multi-departmental focus on Y2K preparations in hospitals; and (3) hospital emergency coordination with other organizations.

The Impact of Y2K on Emergency Preparedness

Study participants indicated that Y2K required extensive emergency planning. The potential for a date-specific failure of technological systems required hospitals to critically examine the shortcomings of their emergency preparedness by significantly reassessing contingency plans, critical-care technology, and emergency supplies.

Contingency Plans: The majority of the thirteen study hospitals indicated that their existing contingency plans were altered in preparation for Y2K. While hospitals are required by the Joint Commission on Accreditation of Health Care Organizations and other regulatory agencies to plan for disasters (JCAHO 2002), hospitals were not prepared for an emergency event such as Y2K. As a result, the study participants reported developing contingency plans to account for the unique aspects of the Y2K threat. Because hospital facilities are comprised of a diverse group of departments, the failure of one of these systems could impact the functionality of the entire system (Delevett 1999). Several study participants observed that the Y2K threat forced hospitals to consider how a localized systems failure could impact the entire organization. As a participant from a California hospital observed:

There are some things out of the box that you have to have up and running from a financial perspective. Then along those lines we determine if the [operating room] is going to be functional, who

depends on the OR? The orderlies depend on the OR. What do you need to make everything a whole?

The Y2K threat required hospitals to plan for emergencies during periods of low staffing. The fact that the transition into the new year would occur during a holiday night shift indicated that employee resources could be somewhat limited. One hospital representative indicated that these off-hour emergency plans were later enacted during a computer failure on the night shift. The Y2K threat also demonstrated to hospitals their dependency on technology. Hospitals observed that the Y2K threat required their organizations to consider operating without computers. As a hospital representative from Tennessee stated:

I think in that same vein, Y2K probably helped us get better prepared, because we looked at every process that goes on in the hospital, and what will happen to this process, if this one doesn't have power or you know if these computers are not available, how are you going to do this process, so we look at every process and how are you going to do it, all the way down to the utilities and everything. How are you going to process the patients, how are you going to process the papers along with the patients and all that.

While none of the study hospitals experienced Y2K related problems, multiple hospitals reported that the Y2K contingency plans were utilized in other emergency events. The plans were enacted in response to small-magnitude internal emergencies; specifically, a flood, a computer failure, and a disruption in water service. The Safety Officer from a California hospital recalled his organization's experiences utilizing Y2K plans in response to an internal flood:

When we looked specifically at the issues that would arise under Y2K, we identified what we would need. You know, potential for the generator to go down under Y2K and the potential that we needed a back up small generator to back up our emergency room. That is where we purchased all that equipment as part of the Y2K. Just right after that in March when [the flood occurred]...and in turn everybody reacted and we went into the internal disaster [mode] and it was just one thing right after another. It was very smooth and we kept the lab up and running. And we were able to move some of our patients to some of the areas.

The hospitals that utilized their Y2K contingency plans in smaller internal events indicated that the plans improved organizational coordination and employee knowledge about safety. Several study representatives noted that their experiences in responding to these events communicated the ongoing value of the Y2K contingency plans.

One study hospital from California indicated that the hospital was revising its emergency plans in order to meet the standards established by the Y2K preparations. As the Director of Support Services from the hospital observed:

[The Emergency Preparedness Committee is] doing some revisions on our management plans....Part of [the committee was involved in] the Y2K Committee, which was a fairly large body also. They developed some really nice emergency preparedness plans. And with that I think there's some things that we wanted to change and implement all that work that went into the Y2K preparation, implement that into our...grander emergency preparedness plans....They're meeting and revising the management plans.

As this observation indicates, for many of the study hospitals, the contingency plans developed for Y2K were not considered irrelevant following the uneventful transfer into the new year. The Y2K

contingency plans were seen by hospitals as applicable to other emergency events, and, as one hospital noted, served as the benchmark for future emergency planning.

Technological Improvements: The threat of technological failure motivated many health care organizations to update or replace non-compliant computers and equipment. The Y2K threat required hospitals to assess the risks of technological failure in their organizations: including, cataloging computer systems; determining the Y2K compliance of equipment; prioritizing and planning equipment replacement or updates; and performing an impact analyses for mission-critical systems and applications (AAMC 1998). For many hospitals the process of assessing risks in technological systems was complex; for example, representatives from a New York hospital pointed out that computers stored inpatient and outpatient information as well as an automated system to order medication.

According to the study hospitals, the threat of Y2K related systems disruptions resulted in the upgrading of critical equipment. The hospitals listed a number of technological equipment that was either replaced or upgraded in order to meet Y2K compliance, including defibrillators, biomedical equipment, personal computers, and elevators. Indeed, many study hospitals expressed concern about the compliance of defibrillators, the medical units utilized in cases of cardiac arrest.

While the hospitals acknowledged that the Y2K threat improved the quality of many mission-critical systems, the study participants observed that budgeting for technological improvements was restricted. Accordingly, focus groups reported that only a few essential items were replaced or upgraded in the hospitals. In fact, a study hospital from New York indicated that it had rented some equipment such as emergency radios in order to save money.

Essential Supplies: In addition to upgrading equipment to meet compliance with Y2K, hospitals also increased the number of essential supplies in case of an emergency. Study participants observed that certain goods and supplies would be critical in a systems failure, and hospitals cited a number of essential supplies that were stockpiled in preparation for the Y2K threat, including medications, flashlights, batteries, bottled water, and antibacterial hand sanitizer.

The majority of hospitals stated that their organizations stored bottled water for use in the case of failures in the public infrastructure. One study participant from a New York hospital made light of the sizeable reserve of water in his facility, “We have enough bottled water to put out the Chicago fire.” Several hospitals indicated that they had not stored bottled water due to internal and external backup sources of water. A few hospitals noted that emergency water could be provided by water towers located on the hospital premises. Representatives from a Tennessee hospital discussed their negotiations with the National Guard for that agency to provide truckloads of water to the facility in the case of Y2K failure.

Because many hospitals increased the supply of non-perishable and general use items, emergency reserves proved to be useful in facility operations following the passing of the Y2K threat. Indeed, many of the items that were stockpiled for Y2K were those that are typically purchased by the hospital. A hospital from New York noted that the increase in essential supplies alleviated the need for the hospital to purchase these supplies for everyday use, thereby making funds available for the next fiscal year. In the hospitals that experienced small internal disasters following Y2K, the reserve of emergency supplies assisted in the organizational responses to these events. Stockpiles of water were utilized in one hospital that experienced a disruption in water services due to an internal

construction accident. As a representative from another hospital that utilized essential supplies in an internal disaster observed, the value of Y2K emergency supplies was demonstrated in that emergency event:

Well, I think with the example of the flood, probably two weeks prior to [the internal flood], the answer would have been, 'Yes, we spent too much money.' The day after [the flood], I think the answer would have been we just spent enough. I think we used every bit of supplies.

Intraorganizational Participation in Y2K Preparedness

Study participants noted that the Y2K problem required a multi-departmental focus in their organizations, and the participation of a diverse collection of individuals, committees, and departments in Y2K preparations. Quite often, hospital safety committees played a central role in developing Y2K emergency procedures, partly due to the pre-existing operational responsibilities of those committees (Brown 1979). However, due to the scope of the threat, the Y2K problem required participation from employees throughout the hospital. Therefore, Y2K was not simply viewed as an information technology problem. Because many hospitals viewed Y2K as a risk management problem rather than strictly a technological problem, the threat was defined as requiring a comprehensive organizational emergency plan (AAMC 1998).

A common theme that was evident in the focus groups was the high level of participation from hospital administrative personnel in Y2K preparations. Some study participants attributed the administrative focus on Y2K to the ambiguous nature of the problem and its potential to cause a significant organizational emergency. A study participant from a California hospital observed that the potential for liability for Y2K damages might have motivated the high level of participation on the part of the administration:

I think it has to do with potential. The administration would surely put more money into earthquake preparedness here than maybe a bomb threat or something like that because of the role of responsibility.

However, a representative from the same California hospital noted that the administration typically participated in emergency planning and safety drills. The administration focus on safety in this hospital may be indicative of a greater focus on risk in California hospitals, due in large part to the region's high seismic risk.

Study participants noted that, in addition to participating in the planning process, hospital administration were an active presence on New Year's Eve. In a hospital from New York, every level of hospital administration was required to report to work on New Year's evening in case Y2K problems materialized. The Vice President of Operations from a Tennessee hospital commented on the importance of administration involvement in Y2K:

We were all here 12 [o'clock] on New Years Eve, every manager that works in this facility was not allowed off. So, I mean that said to the folks, when we are in this situation, these are the things you will have to do and are responsible. Each person had stations in the hospital that they were responsible to go to. And, so I mean everybody understood the impact that could happen.

Interorganizational Preparedness for Y2K

In addition to discussing the intraorganizational focus on Y2K preparations, the hospitals also mentioned the coordination of hospital Y2K plans with other organizations. Hospital emergency planning was defined as dependent upon the level of preparation in the community, other critical care facilities, public infrastructures, and medical supply and equipment vendors. Of particular note were activities that focused on coordination between hospitals and vendors and between individual hospitals and other hospital facilities.

Coordination with Vendors: The hospitals interviewed for the study reported contacting local medical vendors and suppliers in order to determine whether or not technological systems were Y2K compatible. Quite often, the information provided by the vendors served as the foundation for the hospital's assessment of its vulnerability to Y2K. A representative from a Tennessee hospital described this process:

We also got a hold of every one of the vendors or everybody we were doing business with to make sure that they were in compliance. And, if not, what their progress was as a timetable in order to convert their systems to be compliant.

In some instances, the vendors did indicate that equipment was not Y2K compliant, requiring hospitals to purchase new equipment.

Interestingly, one California hospital made arrangements with a vendor to continue receiving essential supplies in the event of Y2K malfunctions. The hospital has decided to continue this arrangement, possibly as a preparedness measure for a seismic event. The hospital's Director of Radiology discussed this process:

Purchasing has stuff set up even as far down as housekeeping supplies. You know just plain old toilet paper can get real important when you don't have any in a disaster. Through the Y2K scenario, material purchasing has developed with their key vendors contingency plan that and we have basically orders placed that if you do not hear from us within an allotted time then you are to ship this order.

Interestingly, the study hospitals did not indicate whether they had tried to determine if vendors were compliant with respect to the Y2K threat. Clearly, a malfunction in a vendor's computer system could have hindered the automatic shipment of supplies to hospitals. Similarly, only one hospital indicated that it had contacted local public utilities about potential disruptions to essential services such as electrical power and water.

Coordination with Other Hospitals: According to focus group interviews, local and state governmental agencies in California and New York attempted to coordinate Y2K preparedness among hospitals. In California, the State Department of Health Services responded to the Y2K threat by organizing the first statewide disaster drills in health care facilities. Representatives from focus groups in California noted that the coordination of emergency drills in all of the state's health care facility was a significant undertaking. As a hospital representative stated:

Realize that California is two states without a boundary, Northern California and Southern California. They don't communicate; they're two totally different states. And to have pulled this off really speaks very great volumes of the State Department of Health Services that they were able to do that.

Following the success of these inaugural statewide drills, the state of California now plans annual disaster drills for the state's hospitals. The focus of the second statewide disaster drill was bioterrorism.

According to the Director of Emergency Services of a New York hospital, the New York City Mayor's Office of Emergency Management was responsible for coordinating the city's hospitals in the event of a Y2K emergency event. The contingency plans stated that the Mayor's Office of Emergency Management was responsible for assessing damages to hospital, coordinating the flow of patients into health care facilities, and communicating with hospitals.

Implication for Earthquake and Natural Hazard Preparedness

According to the focus group interviews, hospital preparations for Y2K resulted in numerous short-term and long-term organizational changes. Clearly, the Y2K threat served to focus hospital attention on mitigating against potential Y2K related risks. The level of Y2K preparedness in the health care industry is notable because natural hazard risk management has typically been a difficult sell for most hospitals. Even in Southern California, where the structural integrity of hospitals has been considerably affected (most significantly in the 1971 San Fernando and 1994 Northridge earthquakes), the adoption of loss reduction measures for natural hazards has met with resistance (Alesch and Petak 2002). In an industry where mergers, acquisitions, and increased competition have highlighted the need for cost reduction, hospitals are less likely to adopt expensive risk management measures (Howe 1998). The organizational resistance to the adoption of loss reduction measures for natural hazards can be effectively understood through Cohen, March, and Olsen's "Garbage Can Model." In this conception, organizational choices are viewed as crowded into a garbage can, where the various problems, solutions, participants, and organizational choice opportunities influence the decision-making process (1972). The garbage can model views choice as embedded in an organizational context of other choices, actors, and relations (March 1978). Clearly, preparation for emergency events must often take a backseat to more urgent financial and organizational issues.

The health care industry's widespread acceptance of Y2K preparation measures raises two important questions. First, what was it that caused hospitals to focus so much on the Y2K threat? Second, why did Y2K have such an impact on hospital operations, when health care organizations continually face natural hazard threats, but do not generally commit significant organizational resources and funds to their mitigation? For example, hospitals in the Central United States prepared for the potential impacts of Y2K; in contrast, hospitals in this region have done little to address seismic risk despite the continual threat of earthquake hazards on the New Madrid fault.

Hospitals throughout the United States devoted significant organizational resources to mitigating the Y2K threat for several key reasons. First, because Y2K was a date certain event, health care organizations were forced to mitigate against its risks in a specified timeframe. In contrast, natural hazard events are difficult to predict, and, as a result, there is rarely a perceived deadline for compliance to mitigation measures. Instead, the mitigation of natural hazard risks is most likely to occur when "windows of opportunity" for policy change present themselves. For example, in the case of earthquake hazard mitigation, the occurrence of high magnitude seismic events facilitates the opening of the windows (Alesch and Petak 1986). Second, Y2K received massive media coverage and scrutiny. The level of media coverage devoted to Y2K is generally not present for natural hazard events. Third, because the Y2K threat had the potential to disrupt the functionality of countless systems, mitigation efforts in health care organization involved the participation of a diverse group

of departments and occupations. In contrast, the responsibility for mitigating natural hazards is typically assigned to disaster coordinators and members of the hospital safety committee. As a result, Y2K was a risk issue that was relevant to entire organizations rather than a specialized department or group of risk decision-makers. Fourth, because existing regulations and codes such as JCAHO safety standards address the mitigation of natural hazards, there is little incentive for organizations to exceed these compliance guidelines. However, the lack of industry-wide guidelines for Y2K compliance required health care organizations to independently assess their vulnerability to the millennium bug. As a result, many hospitals were aware of their vulnerabilities to the Y2K threat and mitigated against these risks. The manner in which hospitals responded to the Y2K problem suggests the potential for these organizations to effectively mitigate against risks. Clearly, if hospitals were inclined to devote the same degree of attention and resources to the natural hazard risks that continually threaten their functionality, these organizations would significantly decrease their risk to seismic events and other hazards.

References

AAMC (1998): Medical schools and teaching hospitals grapple with 'Y2K'. *AAMC Reporter*, <http://www.aamc.org/newsroom/reporter/july98/y2k.htm>.

Alesch DJ, Petak WJ (1986): *The politics and economics of earthquake hazard mitigation: unreinforced masonry buildings in Southern California*. Institute of Behavioral Science, University of Colorado, Boulder, CO.

Alesch DJ, Petak WJ (2002): *The troubled road from adoption to implementation: hospital seismic retrofit in California*. Presentation given at the MCEER 2002 Annual Meeting, Buffalo, NY.

Brown Jr. BL (1979): *Risk management for hospitals: a practical approach*. Aspen, Germantown, MD.

Cohen MD, March JG, Olsen JP (1972): A garbage can model of organizational choice. *Administrative Science Quarterly*, **17** (1), 1-25.

Delevett P (1999): Rx for Y2K: hospitals spending millions. *Silicon Valley/San Jose Business Journal*, <http://sanjose.bizjournals.com/sanjose/stories/1999/02/15/story1.html>.

Giacopetti RJ (1999): *Year 2000 implications for Philadelphia hospitals, health systems and provider organizations*. Delaware Valley Healthcare Council, <http://www.dvhc.org/rr/Y2K.htm>.

Goldberg SH (1997): *Managing 'Year 2000' business and legal risks for hospitals and health care systems*. <http://www.comlinks.com/legal/gold1.htm>.

Howe A (1998): *Millennium bug puts hospitals in intensive care*. http://www.info-sec.com/y2k/y2k_062698b_j.html-ssi.

JCAHO (2002): *Facts about Patient Safety*. Joint Commission on Accreditation of Healthcare Organizations, <http://www.jcaho.org/general+public/patient+safety/index.htm>.

March JG (1978): Bounded rationality, ambiguity, and the engineering of choice. *Bell Journal of Economics*, **9** (2), 587-608.

Whitney DJ, Dickerson A, Lindell MK (2001): Nonstructural seismic preparedness of Southern California hospitals. *Earthquake Spectra*, **17** (1), 153-172.