MANAGING IT BUDGET ANOMOLIES IN THE PUBLIC SECTOR

Dr. Roy A. Boggs, Florida Gulf Coast University, rboggs@fgcu.edu

ABSTRACT

In retrospect, many view the Y2K problem as a challenge that was successfully met, while others proclaim it a vastly overstated media event. Regardless of one's views, IT managers - in both the private and the public sectors - were faced with preparing for whatever it was that was coming. This study takes a look back at how five public sector IT managers responded to budget limitations. It examines how these IT managers addressed, without upper level management budgetary commitment and support, what might have been a catastrophe. Finally, it lists ten 'lessons learned' for public sector IT managers facing anomalies similar to the Y2K problem, foremost of which is the value of multidisciplinary cooperation between users and IT professionals.

Keywords: Y2K, public sector IT, IT management, IT budgets

INTRODUCTION

The transition to the year 2000 created a unique challenge for all organizations relying on technology for continuous operation. It became apparent in the early 1990's that Y2K was not just a problem for big business and major government entities but that it would involve everyone by affecting hospitals, street lights, televisions, airplanes, trains, etc.

Governments at all levels were focusing on Y2K remedies to ensure that mission critical systems continued to function beyond December 31, 1999. Faced with the staggering cost of changing every system that had an imbedded computer chip, and the spiraling cost associated with either replacing the system or recoding millions of lines of software programming, it was not surprising that many outside observers believed it was impossible to fix the problems given the time and resources available. This was especially true for smaller governmental organizations with limited capital resources and small IT staffs.

This report details the results of a longitudinal study examining how IT budget anomalies, as reflected in the year 2000 transition, are managed in the public sector, particularly by local governments. Data were collected and interviews conducted by MBA students as part of a larger research project. The research examines the impact of the Y2K problem on five local government agencies serving a total of over one million year-round residents and two million seasonal guests. The report presents an overview of budgeting difficulties encountered and then discusses how solutions were implemented and which strategies were effective. The report concludes with 'lessons learned' as stated by IT managers.

PURPOSE

The purpose of this longitudinal study is to examine budgeting challenges IT managers in the public sector face when confronted with unique or unusual circumstances. The study is part of a larger study that looks at effects in areas such as personnel, IT resources, and management decisions. The IT community may never encounter another problem identical to Y2K but it is still possible to learn from the situation in order to better manage similar anomalies in the future.

BACKGROUND

The research for this report began in 1998. Data were collected for the budget years 1998 and 1999. Because the overall purpose of the research was to examine the Y2K preparedness of emergency services in governmental entities, hospitals were included as part of the emergency services in the area in which they operate. Specifically, the data gathering centered on the question; "Can our civic leaders assure uninterrupted public safety into the year 2000?"

To answer that question, researchers studied various leadership and management approaches that were being implemented by IT to anticipate and correct Y2K problems. They began the process of describing, comparing, and contrasting the approaches of five governmental entities and two local hospital systems. Of special interest was the issue of budgeting. What will the costs be and how will they be funded?

It was hypothesized that, since private organizations to a very large extent subscribed to a set a six characteristics, these characteristics could be used as benchmarks to assess the preparedness of public entities. Those six characteristics are:

Plan - A written plan should be in place for each department, with specific goals and deadlines for upgrading all equipment to Y2K compliance.

Budget - Adequate funds should be budgeted to meet Y2K compliance.

Committee - A Y2K committee should be formed which has the responsibility of overseeing the Y2K compliance efforts.

Action - The plan should be put into action in a timely fashion through established procedures. Successful Y2K preparation programs should include an informed staff as well as evidence of compliance, i.e. dated completion stickers attached to each piece of equipment.

Testing - Systematic testing of the equipment to ensure Y2K preparedness.

Contingency Plans - Allowances and alternate plans should take into account the probability that at least some systems, both inside and outside the organization, will fail. Plans should be in place to handle the temporary incapacity of suppliers, customers, utilities, and public services.

The second characteristic, budget, soon assumed central importance. Local IT managers were struggling.

Also as the study progressed, it became apparent that the hospitals as a group were quite different and better organized than the governmental agencies in their approach to the Y2K challenge. All of the hospitals surveyed demonstrated a serious commitment to Y2K compliance. All had well documented plans and prescribed corrective programs. Above all, IT was well budgeted for Y2K remediation. It was obvious that top managers and directors in all of the hospitals were very much aware of the possible problems and had made Y2K an important priority. This unique level of performance earned the hospitals a category of their own as a high benchmark against which to measure the local governments. As private agencies with a public focus they were to become the control group.

PROCESS

As a follow-up to the research undertaken above, data were again gathered during the year 2000. These data were retrospective data reflecting what actually happened. Researchers were organized in teams, each with specific responsibilities. For each of the hospitals and public entities, each team conducted personal interviews with the Information Technology managers of a targeted organization. Interviewees were informed that their organization would not be named in the final report. The questions were designed to find out how the problem was managed without compromising any individuals within the organization. Each team had the same set of questions enabling comparisons to be drawn. The specific goal was to find out how the budgeting of the remediation was managed and what effect budgeting decisions had on IT.

Public organizations studied:

A	year-round population	22,100
B	year-round population	49,100
C	year-round population	102,000
D	year-round population	217,500
E	year-round population	429,400
F	control	Hospitals

The interviews attempted to discover where each organization stood in the six areas mentioned in the Background section: Plan, Budget, Committee, Action, Testing, and Contingency Plan. The amount of preparation and level of involvement put into the plan, the thoroughness of the plan, and the timeliness of the plan were all investigated. Finally, questions about the budget were asked. The level of difficulty in attaining the necessary funds was ascertained. The date when funds were made available and the percentage of the total budget were sought. If sufficient funds were not available the effects of the limitations were examined. Once the data were gathered they were compiled and analyzed.

RESULTS

It is now well known that there were no major catastrophes as a result of the Y2K computer problem. There were certainly several minor problems across the country but nothing disastrous happened. This analysis was not done to review the success or failure of Y2K remedies. The objective was to evaluate IT management's response to an expected crisis. Ignoring the problem or failing to solve the problem was not an option for these agencies. Regardless of adequate financial support, IT departments were required to utilize their professional skills to meet their organization's needs and to uphold their public obligation of uninterrupted operations.

Several of the public organizations and their publicly elected officials took the problem seriously and began work before 1998. Others did not even realize that they had issues that might jeopardize their ability to meet their responsibility and protect the population they served until well into 1999. This caused various and sometimes disconcerting problems for the respective IT managers, especially when reviewing and allocating budgets.

The Control Group

In general, the hospitals were well organized and took every precaution to ensure public safety. Top managers and directors became aware of potential Y2K problems before 1997. In the beginning of 1998 they had approved and initiated specific preventative actions.

A Y2K team was formed with members representing all branches of the organization. Formal written plans were created and followed. Employees were directed to devote resources toward preventing possible system failures. Further, funds were appropriated and a Y2K transition budget was provided. The budgets were measured in millions of dollars and represented 140% of the normal annual IT budget. The transition budget demonstrates both the seriousness with which this situation was treated and management's sincere commitment to continued service.

With an ample budget, much effort could be directed towards impeding a potential crisis during pre-millennium days. Plant, equipment, hardware, software, and routine processes were analyzed and ensured to be Y2K compliant. In addition, drills were conducted to simulate various emergency conditions and to test the organizations' readiness. Comprehensive contingency plans were formulated to assist in the event of an undetected noncompliance. In short, the control group performed significant actions to ensure the public's safety and welfare.

The Governmental Organizations

In comparison to the control group, the public organizations studied dedicated little time and few resources to resolving Y2K concerns. Generally, preventative measures began in early 1999; some began much later. In most agencies, transition budgets were nonexistent. All the public organizations researched, with the exception of agency E, made due with only their standard IT

budgets. The percents of the *regular* budget apportioned to Y2K issues are as follows. (Percentages are given rather than dollar figures because the governmental entities serve a wide range of population densities.)

Organization A	15%
Organization B	20%
Organization C	30%
Organization D	30%

Organization E was unique in that it obtained a special budget for Y2K remediation and elected to have a consulting firm perform upgrades and testing. Late in 1998, the agency was prepared to award a bid of 5.8 million dollars to an outside consulting firm with limited knowledge of internal systems for Y2K compliance. The consulting firm wanted an additional 7.2 million to migrate from a mainframe system to client-server system. This contract would have increased IT spending in the agency by 288%. Prior to the contract settlement a group from within the organization submitted a proposal to perform the Y2K remediation *and* client-server migration for just 2.9 million. The internal group completed the work for even less with a final price of 2 million dollars. Expenditures for Y2K remediation resulted in an effective IT budget increase of 23%. This figure represents 0.43% of the organization's overall budget – a small commitment, though better than that of the other organizations.

Since they received few funds specifically for Y2K, public sector IT managers report they were forced to be creative in providing essential services. They did this in a number of ways. All created Y2K committees to research, plan, and make recommendations. Most increased their IT budgets indirectly by asking employees to work overtime hours. This was especially true in the area of testing; all organizations tested during the critical December 31, 1999 weekend. However, it should be noted that expanding one's budget with overtime hours is not comparable to receiving an additional multi-million dollar budget well in advance of the December deadline.

IT managers did what they could with limited funding and their existing workforce. Several used the Y2K crisis as an opportunity to upgrade equipment and software, and to ensure that sufficient maintenance and replacement schedules were established. Most requested support from their user communities creating ties and alliances that remain today. These managers believe that the Y2K situation was beneficial in strengthening teamwork and cooperation throughout their user communities. In addition, several managers used the occasion to draw attention to their understaffed departments and to acquire needed employees.

An analysis of the data suggests that the governmental organizations studied received neither the funding nor the intense backing from upper management that the control group enjoyed. As a result, governmental agencies cut corners, particularly in the area of written documentation; and in general waited longer to respond to the issue than did their counterparts in the private sector.

CONCLUSIONS

It would be inappropriate to assume that public IT leadership considered Y2K to be an insignificant matter. In a public agency it is simply often easier to obtain support for situations

comparable to Y2K after a genuine problem has materialized. Most of the IT managers consulted found themselves left to their own resources and management skills. If they succeeded, and they did, there was little reward. If they failed, they would be alone and responsible. Budget allocation would not be a topic.

Based on the findings of this research, Y2K compliance gained different levels of budgetary support depending on the type of agency. Members of the control group were organized, proactive, and methodical in their approach to this issue. Where the private entities were quick to allocate resources toward preparing their information systems, public IT managers struggled for budgets and support. Budget limitations, as reflected in resources and staff allocations, required IT managers to become resourceful, develop allies and, above all, become politically aware.

Private organizations have CEOs, supervisors, and managers with authority and direct line of command. In the public sector, power is purposely distributed and balanced to protect against individuals acquiring too much control. In absence of legitimate authority and the strong budget planning inherent in private organizations, public sector IT managers have to reach consensus before acting and use innovative means to motivate staff and implement solutions.

LESSONS LEARNED

Top ten strategies for IT general and crisis management in the public sector - compiled from comments made during the interviews with the IT managers.

1. Use functional teams. People working together can accomplish more than individuals working separately. In a governmental agency IT workers are often dispersed. Actively promoting cooperation and interaction helps resolve issues faster and more accurately – quite often at less expense.

2. Develop a budget plan with clear scope. Intelligent budget planning can answer a lot of questions. See item 6 below.

3. Keep a list of current inventory and have a replacement plan, complete with costs. Always be ready! You never know when attention can be focused on the problem at hand.

4. Foster cooperation. Multiple government entities can benefit from sharing work, materials, and programs. The more entities and departments within entities communicate and work together, the more they can benefit from economies of scale, elimination of redundancy, and shared resources.

5. Learn how all of the departments involved in the project, including IT, interrelate. The Y2K anomaly demonstrated how critical a role IT had within all agencies studied. This is essential when presenting budgets.

6. Prepare to justify your decisions and answer to everybody. Publicly traded private organizations must disclose much financial information but not to the degree of governmental

organizations. Documents, correspondences, and budgets are all public record. Managers must be ready to answer budget inquiries by taxpayers and the media and are often under intense scrutiny.

7. If you possess political power, you must apply it liberally and effectively.
When anomalies arise, and they will with some regularity, IT managers in the public sector are often on their own. They rarely can expect the top management support of their counterparts in the private sector.

8. If you do not possess political power, you had better get someone on your side who does.
Reputation and clout often determine who is able to gain support and get things done. Understand that publicly elected officials can be afraid to "stick their necks out" out of fear for public reaction.

9. Become a salesperson. In the private sector, CEOs, supervisors, and managers usually have enough legitimate power that their decisions are not questioned. In the public sector, power is purposely distributed and balanced to protect against individuals getting too much control. In absence of legitimate authority you must use other means to get people motivated and provide needed support. This is especially true for budgets.

10. It's your budget - learn to live with it. When politicians run on platforms of 'more for less', it is difficult for IT managers to convince county and city leaders to provide often critical and necessary budgets. All of the IT managers interviewed were, deep into the years 2000 and 2001, still managing anomalies with limited budgets and staffs. IT budgets in the public sector continue to be limited. However, challenges remain as strong as in other sectors. Successful IT managers in the public sector live with the constraint.