



Y2K COMPLIANCE AND THE DISTRIBUTED ENTERPRISE

It's not just mainframe-based applications: servers and workstations pose significant Y2K problem risks for organizations and individuals.

**J. Arthur Gowan,
Chris Jesse, and
Richard G. Mathieu**

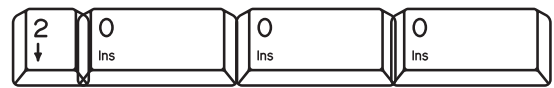
RESOLVING THE PROBLEM OF Y2K COMPLIANCE IS A serious issue for the distributed enterprise. As organizations rely on distributed desktops for decision making and productivity, the risks associated with noncompliant desktops are receiving increased attention from the media, industry analysts, government officials, and corporate leaders. Although most organizations have been aggressively correcting the Y2K problem on their central mainframe applications, many are only beginning to address the significant risks posed by errant desktop software, hardware, and firmware. Since these distributed assets are critical to corporate produc-

tivity, organizations are vulnerable to significant risks if any of the distributed information technology assets cannot properly process four-digit dates.

Consider, for example, investment bankers who issue their first bond trades of the new millennium using noncompliant software. How much will these erroneous trades cost the bank? How much damage will be done before the bank detects and corrects the problem? Now consider all of the critical business decisions that are made based on the data produced by these applications. Given this risk exposure, it is clear that the distributed Y2K problem poses a serious threat to organizations throughout the world.

The distributed enterprise consists of an amalgamation of client and server resources supporting the business objectives of a particular organization. Client resources include PCs and workstations, as well as portable computers such as laptops and palmtops. Server resources include minicomputers and microcomputers. In addition, the distributed enterprise includes the organization's communications infrastructure.

There are three primary points at which potential Y2K-related problems touch the distributed enterprise: intraorganizational-developed applications, shrink-wrapped applications, and hardware/firmware compliance [2]. The first critical step in the Y2K compliance effort is identifying all of the applications, hardware, and firmware in the distributed enterprise. However, since these components are dispersed throughout the enterprise, finding and fixing Y2K problems in a distributed environment is much more complex than in a controlled, centralized mainframe environment.



In order to explore the progress being made in addressing the Y2K problem in a distributed enterprise, a survey was conducted by the University of North Carolina at Wilmington (see "Research Methodology and Demographics"). Specifically, the survey assessed the capability of organizations to correct these problems given their current knowledge of their enterprise, their resources, and their plans for combating the issue. This article summarizes the results of the survey and analyzes organizations' progress toward Y2K compliance readiness.

Key Findings

The survey results indicate that organizations recognize the seriousness of the Y2K desktop problem. The issue is getting attention at the board level, and the vast majority of executives said they would fix the problem before the new millennium. According to the Society of Information Management's Year 2000 Working Group, companies with high CEO involvement in the Y2K problem typically have significantly larger Y2K budgets [3].

- 65% of respondents indicate the distributed Y2K problem is of critical importance to their organizations.

- 91% said that the Y2K compliance issue is receiving attention at the board level.
- 90% indicate that they plan to have all enterprise applications compliant before the new millennium begins.

These responses provide an important backdrop for the rest of the survey results. Although organizations recognize the problem and plan to correct it in time, the survey results reveal that organizations are not well positioned for the new millennium as it pertains to the distributed enterprise.

- 30% of the executives said they do not conduct asset inventories. Of the remaining firms that do conduct inventories, 64% said they are conducting inventories once a year or less frequently. As revealed later in the survey, the distributed enterprise is comprised of a highly fluid asset base; therefore, annual inventories may prove to be inadequate or misleading.
- 68% said their inventory process would not detect the installation of a noncompliant application.
- 31% have not developed a list of noncompliant applications yet, and 9% do not plan on developing such a list.
- 75% have not developed a methodology to ensure that problems are corrected on time and not reintroduced into the enterprise.

These findings raise questions about organizations' Y2K readiness. Given the impending deadline, the number of desktops that may be running noncompliant applications, the lack of asset information, and the lack of compliance progress to date, it is unclear how organizations are going to correct dis-

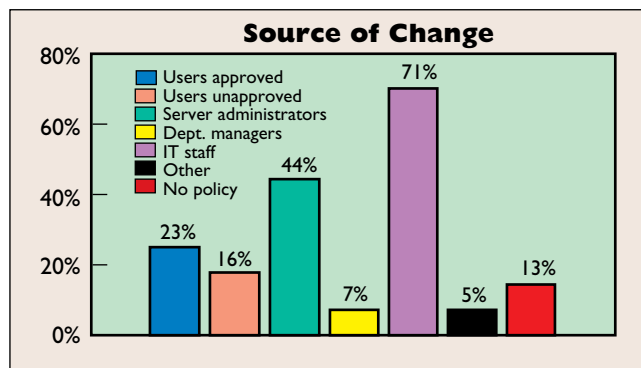


Figure 1. Which individuals are permitted to install software?

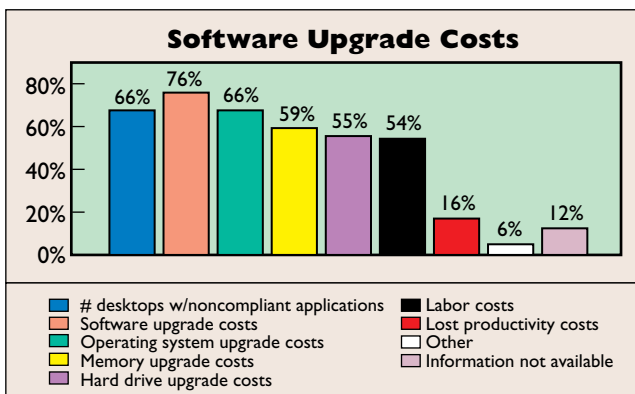


Figure 2. When estimating the cost of upgrading desktop machines in your organization's distributed enterprise, which items do you consider?

tributed systems before the new millennium. If organizations cannot address the problem in time, they face potentially devastating risks, including workstation downtime, dissatisfied customers, revenue losses, and costly lawsuits.

The fundamental first step for organizations involves enterprise knowledge (knowing what assets

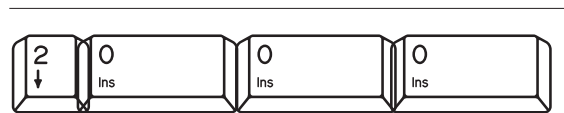
Research Methodology and Demographics

In March 1998, a four-page questionnaire was mailed to 2,773 senior IT executives at Fortune 1000 firms and government entities. The survey questions were primarily close-ended (aided response) and took approximately 15 minutes to complete. The response rate was 18% with 449 instruments returned. This response rate compares quite favorably to other surveys of corporate executives.

From a demographic perspective, we achieved our goal of surveying a representative sample of

Fortune 1000 organizations in the U.S. Respondents to this research effort are senior-level IT executives (Chief Information Officers, Vice Presidents of Information Systems, Information Technology Managers, and Year 2000 Project Managers). The majority of organizations (81%) have more than 5,000 employees, with 8% employing more than 50,000. The annual revenue of 77% of the respondents is greater than \$500 million, with 15% indicating an annual revenue exceeding \$5 billion.

one has). Before organizations can begin to address distributed Y2K problems throughout their organizations, they must know what applications, operating systems, and firmware are installed in their enterprises. However, when asked about the frequency of asset inventories, *30% of the survey respondents do not conduct inventories at all; while 64% of the organizations that do conduct inventories only do so once a year or less frequently.* These are the most compelling results of the survey and uncover a fundamental problem—most organizations are addressing desktop compliance with asset information that is at least a year



must also be able to compare the current number of noncompliant applications to the number of noncompliant applications in the past, to ensure that their risk exposure is decreasing.

- 45% of respondents indicate that software on the typical desktop changes at least quarterly.
- 72% of organizations indicate that their normal inventory process cannot immediately detect the installation of a noncompliant application.
- 31% said they could not determine if the number of errant applications in the enterprise is decreasing or increasing, and 29% said they do not even know whether they can determine an increase or decrease in noncompliant applications.
- 68% of the respondents cannot immediately detect the installation of an errant application.

Organizations that are unable to quickly detect changes on desktops are vulnerable to the reemergence of Y2K problems—even after the correction effort is complete. Furthermore, without being able to track the increase or

decrease in errant applications, it is unclear how managers can verify that they are correcting the desktops at a fast enough rate to meet their compliance deadlines.

Complicating the compliance issue is the fact that there are numerous sources of desktop change. Employees ranging from end users to departmental managers are permitted to install applications, making it even more difficult to prevent the reemergence of noncompliant applications (see Figure 1).

Assessing corporate risks. Another important step in the Y2K compliance initiative is risk assessment, that is determining which desktops are non-

Organization/Description	URL
Yr 2000.Net: several PC/Y2K white papers	www.yr2000.net/members
Federal Reserve Board: testing PCs site	www.bog.frb.fed.us/ly2k/pctesting.htm
National Software Testing Laboratories: PC testing services and white papers	www.nstl.com/html/nstl_y2k.html
PC Magazine: Y2K Resource Center of article, white papers, and utilities, etc.	www.zdnet.com/pcmag/specialy2k/index.html
Computerworld: Y2K Resource Center of articles, venders, discussion groups, etc.	www.computerworld.com/res/year_2000.html
Datamation: Year 2000 manager's Workbench: Many links to other resources	www.datamation.com/Plugin/workbench/yr2000/year.html
Microsoft: Year 2000 Resource Center of white papers, FAQs, services, and tools	www.microsoft.com/technet/topics/year2k/
Everything 2000: go to bottom "Site Map," then "Home PC" for PC/Y2K articles	www.everything2000.com/
Asset Tracking and Y2K Perspectives: white papers on asset tracking and the Y2K problem	www.assettracking.com
Westergaard Online Systems: a series of white papers on PC/Y2K software and hardware	www.y2ktimebomb.com/IT/RL/index2.htm

Table 1. Online resources for Y2K and the distributed enterprise

old—or worse, with no asset information at all. Given the frequency with which workstations and servers are purchased, upgraded, moved, and retired, annual inventories typically become obsolete before the collection process is completed.

Managing desktop changes. Year 2000 compliance requires not only a current view of an enterprise, but also an understanding of how the enterprise is changing. Organizations need to be able to detect a noncompliant application when it is installed. They

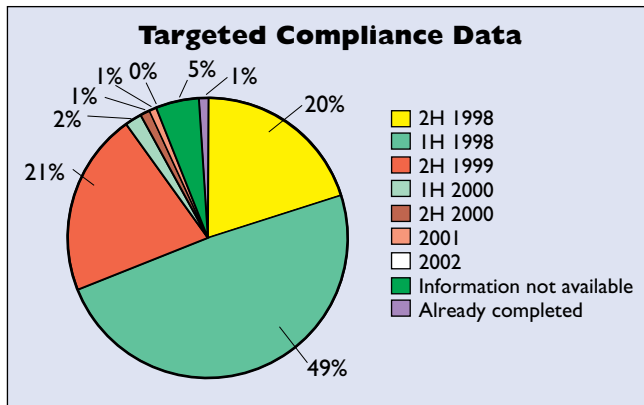


Figure 3. What is your targeted date for ensuring all enterprise applications are Y2K compliant?

compliant and understanding the importance of those applications to the corporate mission. It is imperative that all companies develop plans to address distributed system Y2K risks. These should incorporate many tasks that apply to mainframe-based Y2K projects, but must be adjusted for the distributed enterprise [1].

Year 2000 planners must also create and follow a methodology that involves several steps: examine the top applications in the enterprise, determine which ones are noncompliant, and then evaluate the importance of those applications to the organization, thereby minimizing risk exposure as much as possible. However, according to the survey results, most organizations are only in the early stages of this process:

- 31% of the executives have not yet developed a list of noncompliant applications, while 9% do not plan on developing such a list.
- 35% of executives indicate that between 10% and 50% of their enterprises are running noncompliant firmware (BIOS versions).

- 42% have not ranked the importance of noncompliant applications to the organization, and 22% do not plan on ranking this importance.
- 45% have not quantified risk by department.

Without performing these preliminary assessment steps, it is unclear how organizations can devise correction plans that will minimize their corporate risk exposure. Furthermore, the survey results indicate that organizations do not have a complete understanding of which desktops are noncompliant.

Calculating Y2K correction costs. When correcting noncompliant desktops, hardware and software upgrades are often required to support the new compliant applications. The average estimated correction cost was reported to be approximately \$340 per desktop, but 30% of the respondents indicate that they do not have sufficient information to make an estimate. Additionally, when budgeting for application upgrades, ancillary costs, such as lost productivity, are often overlooked (see Figure 2). The implication of these findings is that initial Y2K budgets will be inadequate to cover the final compliance price tag.

Securing resources. Of the organizations surveyed, 30% have not yet secured the resources necessary to address compliance before the new millennium. Some experts claim that as many as 15% of all businesses will face bankruptcy due to a lack of operational funds or Y2K legal liabilities [4].

Given that many IT departments are understaffed and/or fully applied, the distributed Y2K compliance effort will, in most cases, require external resources. Only 22% of surveyed companies will rely solely on their internal staff, while 75% will be augmenting their staff with external resources. Most reported using independent consultants or systems integrators. These results reveal organizations' vulnerability to resource shortages and escalated labor

The Status of Each Y2K Compliance Step

Problem Identification—65% of the respondents have located errant applications within the enterprise.

Risk Assessment—54% have assessed corporate and departmental risk exposure from noncompliant applications.

Risk Correction—35% have calculated the cost of correcting errant workstations and servers, including the application and various component costs.

Compliance Planning—29% have determined which desktops to fix and in what order.

Compliance Modeling—17% have concatenated (or linked together) various compliance fixes to produce the net changes required for each targeted desktop.

Risk Management—25% have developed a methodology to ensure that problems are corrected on time and are not reintroduced into the enterprise.

rates. As the deadline approaches, external resources may become more difficult and expensive to hire, thereby making the Y2K compliance effort even more costly.

Developing a Y2K compliance methodology.

Although specific Y2K compliance methodologies have been defined and are readily available for central mainframe applications, few methodologies have been published to guide organizations through desktop compliance initiatives. Perhaps this is why the executives surveyed indicate they are only in the early stages of defining and implementing a desktop compliance methodology as shown in the sidebar “The Status of Each Y2K Compliance Step.”

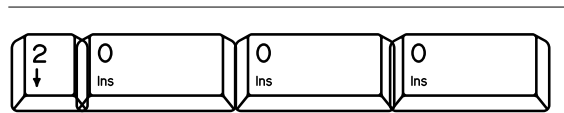
These results reveal that most organizations have only completed the preliminary steps in the compliance process—that is, they have begun to identify errant applications and to assess their risks, but the majority of executives have not made significant progress past this step. To manage the problem, inventories of hardware and software must be completed and then triaged on the basis of risk [5].

Y2K compliance goals vs. Y2K compliance readiness. Most executives (80%) say they will have sufficient funding and human resources to fix the majority (76%–100%) of their noncompliant desktops by January 1, 2000. However, other responses in this survey call into question the executives’ funding and resource expectations. For instance, 65% of the respondents have not performed a risk correction analysis (calculating the cost of correcting errant desktops). In addition, 30% have not identified and secured the required resources. Given these results, it is unclear whether organizations will have sufficient funding and resources to ensure desktop compliance on time. Other doubts are raised by the anticipated date for ensuring that all enterprise applications are Y2K compliant. Seventy-one percent (71%) of the respondents said they will be compliant by the first half of 1999, which is approximately one year from the time the survey was conducted, and 92% said they will correct the problem before the start of the new millennium (see Figure 3).

How will these organizations be able to ensure compliance within 12 months when 20% acknowledge they do not know the percentage of desktops that are noncompliant? Over 70% have not even developed a compliance plan, and the plans that have been developed appear to be based on questionable data.

Conclusion

The survey results reveal a serious problem—the majority of organizations believe they will correct



noncompliant Y2K desktops before the new millennium; however, they do not have the methodology, information, or sufficient budgeted resources to do so. Specifically, the majority of organizations do not have accurate asset information to identify noncompliant desktops, they have not determined which desktops to fix and in what order, and they have not developed a methodology to ensure that problems are corrected and not reintroduced into the enterprise. The distributed environment is dynamic, seriously complicating the compliance maintenance process.

Given the tight deadline, the desktops that may be running noncompliant applications (especially those supporting critical applications), and the limited progress that has been made, it is unclear how organizations are going to protect their employees, shareholders, and customers from the potentially devastating effects of noncompliance. ■

REFERENCES

1. Hayes, I.S. and Ulrich, W.M. Distributed systems challenge: Are you ready? *Software Magazine*, (July 15, 1998), 22–28.
2. Jesse, C. *Teaching Chipmunks to Dance: The Business Leaders' Guide to Making the Distributed Enterprise Year 2000 Compliant*. Kendall/Hunt Publishing Company, Dubuque, IA, 1998.
3. Kappelman, L.A., et al. Calculating the cost of Year-2000 compliance. *Commun. ACM* 41, 2 (Feb. 1998), 30–39.
4. Nolan, R.L., et al. Connectivity and control in the Year 2000 and beyond. *Harvard Business Review*, (July–August 1998), 149–166.
5. Orenstein, D. Desktops are not immune to year 2000. *Computerworld* (July 13, 1998), 53–54.

J. ARTHUR GOWAN (gowanj@uncwil.edu) is an associate professor in the Cameron School of Business at the University of North Carolina at Wilmington.

CHRIS JESSE (chrisj@tangram.com) is the president and CEO of Tangram Enterprise Solutions, Inc. in Cary, North Carolina.

RICHARD G. MATHIEU (mathieur@uncwil.edu) is an associate professor in the Cameron School of Business at the University of North Carolina at Wilmington.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.