5-1997

Members in Finance and Accounting, May 1997

American Institute of Certified Public Accountants (AICPA)

Members in Finance and Accounting

May 1997

AICPA

Assessing Year 2000 Vulnerabilities— A CPA in Finance & Accounting Concern

Highlights

Robert R. Moeller
President, Compliance & Control Systems
Associates, Inc.
Evanston, IL

One thousand years ago, Christian religious leaders in Western Europe fervently preached about the then upcoming "end of the world." Based upon historical accounts, there was much frantic talk and dire predictions about the Year 1000. Despite all of these prophesies, we are still here. We are again on the eve of a new millennium, the Year 2000. The current warnings about the consequences to our computer systems and to our businesses because of the Year 2000 sound almost as perilous as those of the prophets 1,000 years ago.

The Year 2000 may cause major problems in many organizations. The problem is caused by the way dates were established in computer programs written over the years. To allow for the easy calculation of interest and other time sensitive matters, dates were often set up as a numeric YYMMDD value. The two YY characters were used for the year rather than YYYY to save computer memory, thinking the year 2000 was too far into the future. This date description may cause problems whenever a computer program calculates such things as future employee benefits. Today, a computer program might compute a future benefit by adding years to a current date, such as 970415. Come the year 2000, this date would become 0415 and calculations based on subtracting days could produce unpredictable results.

This Year 2000 problem presents a challenge for the CPA in industry. Date related programs can be critical for long term interest, inventory aging or employment benefits cal-culations. While much of the work in correcting this Year 2000 problem will be the responsibility of the information systems function, the CPA in industry is a financial manager who should take a lead in determining the extent of the problem.

A review can take place in three phases. First, assess what actions information systems and others in the organization have done to date about Year 2000 problems. Second, understand the extent of the problem and third, working with the management team, develop a plan to correct any Year 2000 threats.

When asking Year 2000 questions, the CPA may encounter a variety of responses ranging from "we don't have a problem!" to "we plan to attend a seminar," to strong action plans to correct the problem. The "no problem" response is almost always unacceptable unless the organization has done a detailed analysis of its vulnerabilities. That assessment must go beyond the organization's basic busi-

Other Supplements Available

All supplements produced with the May issue of *The CPA Letter* are available via the Internet after May 15, and on the AICPA Fax Hotline.

www.aicpa.org/pubs/cpaltr/index.htm

201/938–3787; document no. 1550 large firms, 1551 medium firms, 1552 small firms, 1553 business & industry, 1555 internal auditors, 1556 government, 1557 education, 1566 practice alert (ERISA audits).

ness data processing systems and include all computer systems.

The next step in assessing Year 2000 vulnerabilities is investigate all potential problem areas. Too often, concerns are limited to just the 6 character YYMMDD format dates. Other manual and automated systems may encounter problems. Solutions are often difficult because YYMMDD dates were often coded into computer programs many years ago, and both the programmers who wrote them as well as supporting documentation are often long since gone. Specialized software is available to help solve these problems, and some organizations have resorted to a line by line reading of program source code to find problems.

Working with members of information systems and others in management, the CPA should develop an inventory of which systems depend upon these YYMMDD dates as well as how they impact external sources including suppliers and other agencies. This can be a major and expensive problem for all concerned. The CPA should then use these findings to help develop a formal action plan to correct the problem.

The Year 2000 is coming and is an immovable deadline that can not be missed. CPAs in industry can provide some very effective support to their company by assessing the corrective actions necessary to meet this deadline. A Year 2000 vulnerability review is an important activity that can provide some important information for further actions.

Software Asset Management: Why You Should Care About Software Piracy

From its introduction over 20 years ago, the PC has forever changed the way we do business. As a result of huge technology advances and a highly competitive market, technology costs have plummeted and a PC on every desktop is a reality.

In small businesses, where no prior computer technology existed, PCs have evolved from a collection of isolated workstations to an integrated PC network. In larger businesses, PC networks have replaced or supplemented existing mainframe or minicomputers. In all businesses, PCs, minicomputers and mainframes are becoming a part of the mother of all networks, the Internet.

This distributed computing model increases the benefits of technology by bringing information closer to the knowledge worker and end-user. At the same time, this decentralized approach is inherently more challenging for technology professionals to manage and often results in unknown and uncontrolled costs of ownership.

One factor that contributes to this uncontrolled cost is the lack of software standardization across the enterprise. Business PCs usually start their service life in an approved configuration but over time get modified through software upgrades and installation of non-approved user software. Eventually, no two PCs are alike.

Some of this is to be expected but lack of an enforced standard creates a support challenge for information system personnel and encourages end-user practices that are not in the best interest of the enterprise. Some of these practices include:

- decentralized software purchases
- copying company software for home use
- installing unauthorized software of unknown origins (that may be infected with viruses)
- installing software on multiple workstations when only one license exists.

These practices increase support costs and lead to possible under or over licensing of software. You may be surprised to hear that you are over licensed but if you don't know what's installed on your workstations, you just don't know. By keeping track of software and licenses, you will be assured that you are paying for only the software you need. On the other hand, the cost may be more significant if you are under licensed.

The Costs of Software Piracy

Each year, the software industry loses an estimated $12.8 billion due to software piracy. The software industry takes this problem very seriously and has created the Business Software Alliance (BSA) and the Software Publishers Association (SPA) to police the illegal use of software. Both organizations have a toll-free number for whistle-blowers that is well publicized and gets used a lot by disgruntled employees. Following are some recent examples of actions taken by the BSA that resulted in some hefty penalties:

- A $325,000 penalty paid by Professional Service Industries Inc., a Chicago-area engineering consulting firm
- A $175,000 penalty paid by Massachusetts-based Memotec Communications Corporation
- A $160,000 penalty paid by Enterprise Products Company, a petro-chemical company headquartered in Houston
- A $97,500 penalty paid by Electronic Measurements, Inc., an

engineering firm in Neptune, NJ
• A $77,000 penalty paid by Ironstone Group, Inc., a real estate tax consulting firm headquartered in San Francisco.

Regardless of intent, if your company is using software that is not covered by a license, it is considered pirated software. The unauthorized use of software is frequently the action of careless and isolated individuals and usually does not reflect management policy. If caught, you or your company could be tried under both civil and criminal law. A civil action may be instituted for injunction, actual damages (including infringer's profits), or statutory damages up to $100,000 per infringement. Criminal penalties include fines up to $250,000 and jail terms up to five years, or both. In many cases, as in those noted above, the company agrees to a financial settlement but may also incur legal fees, negative publicity, and possible business disruption from the loss of key business software.

What Should You Do?

Your first responsibility as a software user is to purchase original programs only for your use. If you purchase software for business use, every computer at your place of business must have its own set of original software and the appropriate number of manuals. It is illegal to purchase a single set of original software to load onto more than one computer or to lend, copy or distribute software for any reason without the prior written consent of the software manufacturer. You should have the following procedures established for your organization:

• Prepare an annual analysis for your organization to determine what software is needed. As a general principle, the analysis should answer some basic questions: Is the organization using the most efficient and effective software to meet its needs? Is the staff satisfied with their current software packages? Are there other packages which would enable your staff to operate in a more proficient manner? Identify the appropriate software profile for each computer user by assessing whether departments or individual staff members need alternative or extra software packages. Network operators should consider purchasing a network metering package to restrict the number of users according to the number of licenses.
• Prepare an inventory of your current software with licenses and conduct periodic physical checks to determine compliance. Any illegal software discovered during the inspection should be deleted right away.
• Purchase licenses for enough copies of each program to meet your current needs. Budget for buying future software to keep up with your staff requirements.
• Demonstrate your organization's commitment to software management and use of legal software by adopting appropriate procedures. For example, appoint a software manager to ensure that all the software analysis and management functions are conducted efficiently; create and circulate an antipiracy policy to all employees; and communicate with all organization staff reiterating the organization's recognition of the concern about software management.

For further information, you can contact the following organizations that specifically address software management and piracy.

Business Software Alliance, 1150 18th St. NW, Suite 700, Washington, DC 20036, tel: 202/872–5500. Web site: www.bsa.org.

Software Publishers Association, 1730 M St. NW, Suite 700, Washington, DC 20036–4510, tel: 202/452–1600, Fax-On-Demand Service: 800/637–6823. Web site: www.spa.org.

US and UK Views on the Accounting Trends

Robert Sweeting, Professor, Manchester School of Management, UMIST, UK;
John Fisher, President, New Finance Associates, Newton Center, MA;
John Morrow, Director, AICPA, NY

Much is being written about "The New Finance" and its function. The AICPA and the Institute of Chartered Accountants of England and Wales have been actively involved in seeking out from their members and informed commentators their views on what the shape of accounting generally will look like in the year 2000 and beyond. Many organizations are undergoing major change because of the impact of delayering, shifts towards boundaryless businesses and closer integration with suppliers and cus-tomers. Because of supply chain networks, most types of businesses are involved. These are businesses where cost reduction, speed, flexibility and "delivery delight to customers" are seen to be essential.

Accountants everywhere are now required to add value and not merely to operate as bean counters. They are being exhorted to integrate and partner with colleagues in developing and leading new ideas and cannot be satisfied to be only followers. Inevitably, questions have been asked about how management control requirements can be balanced against the spin-offs from the different kinds of corporate innovations that are being put in place. An impetus for this questioning has been highlighted by recent well publicized failings in corporate gover-nance in the US and European led businesses—not all of which businesses have survived intact. Accountants therefore walk a narrow line between moving with the times and ensuring what is in place supports financial integrity and viability.

The Survey

What follows is the result of a survey amongst 74 US and 16 UK senior accountants based in a range of organizations: manufacturing and service, large and small, for-profit and not-for-profit. The data was collected by questionnaires completed by accountants in the US from a fax survey questionnaire of readers of the May 1996 AICPA *Financial Manager's Report* and in the UK from attending focus group meet-

Table 1

US AND UK FINANCE MANAGERS RANKING OF ACCOUNTING TRENDS

ACCOUNTING TRENDS	Importance	Agenda Priority	Implementation in my organization
The sudden emergence of truly global capital and investment markets, coupled with innovative and challenging financial schemes and business practices, places enormous pressures on finance to keep up in managing and measuring value risk and return	6	7*	2
An acute and growing demand on accountants to supply strategic decision support information as a crucial competitive weapon	2	2	4
Rapid acceptance of desktop and network information technology as both the enabler and driver of change	1	1	1
Fundamental and massive changes in how transaction processing, recordkeeping and basic financial reporting are accomplished	3	4	6
A greatly enhanced and expanding role of finance as overall business leaders and strategic business partners	4	5	3
Dramatic shifts in organization and human behavior systems towards flat management structures with informed thinking, empowered and accountable workers	5	3	5
Almost entirely different professional tools, skills, roles, people and behavior	7	6	8
Heightened anxiety and challenge about the crucial issues of accountability, control and governance	8	7*	7
	Ranking 1=Highest	Ranking 1=Highest	Ranking 1=Highest

*Ranked The Same

ings. The respondents were asked to give their views about how important they believed the suggested list of key emerging trends (see table above) are, their agenda priority and their experience of them.

Respondents' Feeling
The questionnaire provoked some respondents to express their general feelings:

"Many of the trends are occurring simultaneously with some of the trends opposed to other ones. How it settles out over the next 2–3 years will be very important to progress in the finance function."

"The resources and training necessary to move to the 'leading edge' are prohibitive."

"Training on the trends issues is critical. Unfortunately, demands in the corporate environment have gotten so much, there is little time for training."

"I was surprised others were thinking just as we are about these issues."

"Some of the same demands on for-profit companies are appearing on the doorsteps of not-for-profit entities such as ours."

"Accounting and finance are some of the most heavily relied upon departments (in the business) for information, insights and innovation."

Respondents also offered insights into what they were doing to bring about change:

"You are right on the mark with each trend you've listed. Our angle on solutions has been two pronged. First, we've stopped doing a lot of recordkeeping and reporting deemed unnecessary. Second, for the work that remains, we've been leveraging people with technology to maximize productivity."

"Of primary importance is to provide a stewardship function control and accountability of assets, income and expenses. Next in line is to provide strategic decision-making support. Then to provide measurement statistics of value, risk and return."

The Way Forward
Our poll has suggested that there may be some differences in emphasis in handling the set of trends identified, between US and UK accountants. To some extent these differences may be explained in terms of comfort with new technology and existing competencies. There was certainly little complacency that was observed in the poll findings. In fact, there were serious concerns about the need for substantially enhanced and ongoing training required to handle a much changed job. However, there were questions about where the resources

were going to come from to pay for this in terms of both money and time. All this points to a need, therefore, for better understanding, development and dissemination of improved mechanisms and processes to facilitate and effect the changes. The dangers of not doing this are immense, with people left to fumble along with half truths and misunderstanding. All of which will frustrate wider business improvement initiatives.

New Practice Alert
Members should be aware that along with this month's *CPA Letter* is a practice alert on ERISA (Employee Retirement Income Security Act) audits. The alert covers the deficiencies noted by the AICPA self-regulatory teams and by the US Department of Labor in employee benefit audits. The practice alert describes how to find guidance to avoid such deficiencies and how to obtain information on best practices in ERISA audits.