

TECHNOLOGY IN THE YEAR 2000 AND BEYOND

**Al “VirtuAl” Harrison
Harrison & Egbert, Houston
VirtuAl@hypercon.com
<http://www.allegal.com>**

**1999 CPE TAX EXPO
Texas Society of Certified Public Accountant**

Houston Chapter

TECHNOLOGY IN THE YEAR 2000 AND BEYOND by Al Harrison

Technology in the Year 2000 will enable practitioners to experience many of the myriad benefits of computer technology. Is the paperless office attainable yet? Has computer technology advanced far enough to enable information to be transported and transmitted wholly electronically? Is it now possible to transfer data by voice input accurately at normally speaking rates? How has the exponential growth of Internet travel promoted communication of electronic documents? While engaging in such communications, what prophylactic measures should the practitioner take to assure confidentiality and to avoid invasion by viruses and the like? Ironically, the Year 2K “bug” — attributable to past representation of dates by only two digits — has accentuated awareness of data protection and security issues. Let us consider how these and related issues will affect the professional office in the Year 2000 and beyond.

Paperless Office

While working in a paperless office is probably not attainable in the Year 2000, steps may be taken to enable this “paperless” state to be asymptotically reached during the New Millennium. Thus, as a means for achieving a paperless state, an office must first become comfortable with a “paperlite” state. A paperlite state is contemplated to be characterized by a professional such as a CPA gradually increasingly using documents in electronic form and storing information in electronic databases. Thus, under this environment that purports to transition an office ultimately into a paperless condition, paper documents become a disfavored medium of communication.

To sanely function in a paperlite office, a practitioner must adjust to routinely not handling paper. Surfaces of desktops and perhaps credenzas are no longer obscured by piles of paper and file folders. Unfortunately, these surfaces may still be obscured — but by objects other than paper documents. Sound impossible?

Consider the ensemble of hardware and software tools that are prerequisite for enabling the paperlite state to be realized. First, of course, there must be a suitable hardware and concomitant operating system platform that provides the landscape for accommodating electronic communications and storage of electronic databases. Basic computer hardware includes current-generation stationary desktop computers (“towers” and “mini-towers”) and portables (“notebooks”) provided with sufficient computing power (minimum of 200 MHz, 64 megs RAM, 8 megs VideoRAM, 8 gig hard drive, 32X CD-ROM drive, accelerated graphics, etc.) and with large display screens (at least 17" monitor for desktops and 12" for notebooks).

The hardware environment should preferably be implemented in a local area network configuration that is easily extended using notebooks and even handheld portables (“palmtops”) that should be inherently synchronized with the networked office computers. Indeed, such portables may be construed as constituting part (not an extension) of this paperlite office environment.

TECHNOLOGY IN THE YEAR 2000 AND BEYOND by Al Harrison

Next, besides hardware, the platform must in an operating system for enabling the hardware to conveniently and reliably work with peripheral devices (modems, printers, scanners, etc.) and with software applications. The recent incarnations of Microsoft Windows (Win 95, Win 98, Win NT/2000) have delivered graphical, generally user friendly interfaces, but have provided users insufficient reliability and stability. The Apple Macintosh operating systems have typically been more reliable than Windows, but have had much less applications commercially available. In Year 2000, the Linux operating system will afford a more reliable and stable platform than ever offered by Microsoft. Competition from Linux, and perhaps in conjunction with the government prevailing in the current antitrust lawsuit against Microsoft, will provide incentive for Microsoft to finally deliver reliable operating systems — friendly not only to users, but also to other vendors.

Instead of an office being permeated by conventional paper flows and accumulations, there now is a multifaceted electronic flow of information. Forms may be retrieved by being downloaded from the Internet, by being copied from E-mail attachments, and by being copied from CD-ROMs. What happens to the retrieved forms? Are the forms completed electronically, i.e., by editing in word processors or other application software, and then transmitted to the client or the government? On the other hand, are the forms printed on paper (a step backward from the paperlite office) and then completed using a typewriter and forwarded to the client or government via regular or overnight mail? What do the paper and electronic audit trails compare? Can fail-safe electronic audit trail and backup procedures be reasonably established? How can paper documents be metamorphosed into electronic form? How about voice input? How should documents be transmitted electronically? Should encryption be used? Does color and sound matter?

Separate from storage, retrieval, and transmittal of electronic documents, the paperlite (and, of course, the paperless) office must have the benefit of an information monitor and manager that has immediate access to cross-tied information relative to virtually every aspect of a professional's practice. Clients must be cross-tied to their files; both client and associated files must, in turn, be tied to every related task and event. Practitioners' tasks and events must be calendared with a concomitant tickler or reminder system to warn when due dates are approaching. Date-stamped electronic note-generation must be enabled to avoid resorting to paper notes when clients call or visit the office. Are products available that offer some or all of these functions and features?

Representative Meritorious Software:

Adobe Acrobat
Caere OmniPage Pro
Corel Presentations, WordPerfect
Data Text Time Matters
Dragon NaturallySpeaking

TECHNOLOGY IN THE YEAR 2000 AND BEYOND by Al Harrison

Gold Mine
Inso QuickView Plus
Lernout & Hauspie VoiceExpress
Microsoft Power Point, Word
Mijenix Fix-It! Utilities, PowerDesk, ZipMagic
Network Associates Virus Scan, Dr. Solomon's Antivirus, First Aid, PGP
Powersoft DriveCopy, ImageCopy, Lost & Found
Qualcomm Eudora Pro
Sage Group Telemagic, Timeslips
Symantec ACT!, Norton AntiVirus, CrashGuard, Ghost, pcANYWHERE, Utilities, WinFAX
Teal Software
Trellix Software Trellix
Xerox TextBridge Pro

Representative Meritorious Hardware:

3COM Palm III
Imation Super Drive
Iomega Zip Drive
Labtec Audio/FX, Headsets
Microtek ImageDeck
Norcom (Handheld) Dictation Interface
VXI Headsets

Accessing Documents & Information On-line

Site Name	URL	Description
Code of Federal Regulations	www.access.gpo.gov/nara/cfr/cfr-table-search.html	search engine for CFR
Federal Web Locator	www.law.vill.edu/fed-agency/fedwebloc.html	links to federal Web sites
Fedworld	www.fedworld.gov	links for searching and locating government-related information
Internal Revenue Service	www.irs.ustreas.gov	IRS forms and publications
Securities & Exchange Commission	www.sec.gov	access to EDGAR

TECHNOLOGY IN THE YEAR 2000 AND BEYOND by Al Harrison

Data Protection and Security

One subtle, perhaps unanticipated, benefit of the Year 2K scenario, is that the potential for data-related confusion and data-loss has heightened practitioners' awareness of the criticality of regularly assuring the integrity of corporate and client data. Files and or file-folders should be backed-up on a routine basis. Fundamentally, files may be stored on a diversity of storage media including vanilla diskettes, Zip disks, Super-disks, tapes, removable hard drives, and CDs. Backup procedures may exploit the Internet by storing files on secure Web sites; similarly, these procedures may include redundantly storing files or folders on local area networks.

For instance, a simple Windows 95 or Windows 98 peer-to-peer network — immediately activated by physically interconnecting network-ready computers — may store multiple copies of folders on different networked-computers. Backup data should also be stored off-site to be available for restoring files if the integrity of office computers is somehow undermined due to weather, power failures, etc. Notebook computers and even the Palm III Connected Organizer may be used as a source for restoring damaged files. Before a back-up operation is considered complete, verification should be conducted.

Regardless of how or where data is stored, security is an important concern. Computers may be easily password-protected to prevent unauthorized access. If portable computers are lost or stolen while traveling or otherwise, sensitive data may be inadvertently disclosed. Data security may be accomplished at the hardware level by “locking” keyboards and screens. Security may be accomplished at the software level by password-protecting or encrypting particular files.

An essential ingredient of a safe computer system is an anti-viral “shield.” Viruses, unfortunately, are readily transmitted to hard drives by infected diskettes, Zip disks, or other portable media and also via downloaded files. An anti-virus application should preferably be running in the background to be constantly on-guard for viral invasion.

Representative Meritorious Software:

Data Text Time Matters

Mijenix Fix-It! Utilities, PowerDesk, ZipMagic

Network Associates Virus Scan, Dr. Solomon's Antivirus, First Aid, PGP

Powersoft DriveCopy, ImageCopy, Lost & Found

Symantec Norton AntiVirus, CrashGuard, DiskLock, Ghost, pcANYWHERE, Utilities

Teal Software

TECHNOLOGY IN THE YEAR 2000 AND BEYOND by Al Harrison

Year 2K Scenario

Of course, the advent of Year 2K promises to minimally cause excitement and maximally to deliver chaos to the industries across the board. This anomalous situation arises due to two-digit year coding of date-related fields. Concomitant anomalies arise due to leap year coding and "999" (default) coding. The two-digit year coding problem occurs when computer clocks, read-only memory, and operating system and application software refer to year via the last two digits — excluding the first two digits, i.e., "98" instead of "1998." If computer components in hardware or software cannot distinguish the year 2000 from the year 1900, based upon a year of 00, then operation of the computer may abnormally terminate or unpredictable results may occur. Interestingly, under Year 2K conditions, an IBM-compatible computer may revert to a date of January 4, 1980, corresponding to the genesis of the Microsoft DOS operating system.

The leap year coding problem arises under pathological circumstances: while 00-years are ordinarily not leap years, 2000 is, indeed, a leap year. Such a leap year aberration has not occurred since 1600! Many programmers in the 1960s and 1970s were clueless about Y2K having a 29th day in February. The 1999 coding problem occurs with software that uses a year of "99" to signal when certain archived data and the like is set to expire. This was simply an "idiot-proof" convention assumed by system designers and programmers to represent the latest date (in the distant future) that could be used to as an expiration date. Depending upon the computer program code, such files may expire on 9/9/99 or 1/1/99.

There are several approaches for coping with the potential impact of Y2K fallout. Perhaps the most conservative is to simply set the system clock back 30 or 60 or 90 days, as appropriate, and observe what happens to the outside world. Any artificial dates automatically appearing on correspondence and other documents must be manually adjusted to the correct date. The brave, opposite approach is to set the system clock ahead to just prior to Y2K, and then observe if any deviations from normal office computer operations occur. Of course, all important data should be (double) backed up prior to entering this brave new world.

Representative Meritorious Software:

Intelliquis Fix 2000
Symantec Norton 2000

Representative Meritorious Hardware:

Intelliquis Fix 2000

TECHNOLOGY IN THE YEAR 2000 AND BEYOND by Al Harrison

Communicating via E-Mail and Traveling on the Web

Many practitioners have discovered the benefits of communicating online with colleagues and clients. Similarly, many practitioners are intrigued by the “Wild West” nature of the Internet and enjoy exploiting the seemingly unlimited resources available on the Net. Obtaining a diversity of readily available multimedia information throughout the World Wide Web, passively or actively participating in relevant Newsgroups and ListServes, and downloading files and documents — directly or indirectly — via FTP, professionals traveling from their desktops into Cyberspace have experienced the myriad opportunities to become the virtual center of a circle of an amorphous, unending universe.

To enjoy the fruits of the Internet, however, practitioners and their support staffs must appreciate the several hazards associated with traveling in Cyberspace. For example, while attempting to retrieve information relevant to a particular matter, practitioners frequently use directories and/or search engines to navigate throughout an inherently chaotic, disjointed collection of databases stored on file-servers. The location of these databases is of no moment: all that matters is that appropriate sources of pertinent information are located, browsed, and then downloaded or otherwise obtained as appropriate. If such information is not properly retrieved, e.g., if searches are improperly defined to one or more search engines or if directories fail to point Net research in the correct direction, then important information may be missed. Similarly, identifying suitable Newsgroups and ListServes via appropriate directories and search engines may miss opportunities to learn crucial information about matters of import to the firm. The use of meta-search engines, that inherently and sequentially invoke multiple search engines (and automatically pass the specified search criteria in proper format to each engine) help obtain sought-after information.

As another example, while being a profoundly convenient means for communicating independently of time and geographical limitations, E-mail may introduce significant risks of breaching client confidentiality or disclosing proprietary information to third parties. E-mail messages, which are frequently prepared impromptu, may be another vulnerability for professionals. The tendency to respond to virtually all E-mail messages may inadvertently drive practitioners to deliver unengaged professional services. Similarly, such impromptu E-mail may elicit communication that was relied upon for financial or tax advice, while merely being intended to be an off-the-cuff commentary. Sound travels fast on the Net.

It should be noted that the delivery of E-mail across the Internet typically implicates routing of information packets across a plurality of file-servers which may be operated by diverse entities including commercial businesses, academic institutions, non-profit organizations, etc. A practitioner sending an E-mail to a client has no control over the routing of the message pursuant to arrival at the specified destination. That is, a typical E-mail message — from a practitioner to a client — is routed over a sequence of physical file servers / computers which are beyond the sender's control. As this message engages each computer of such a sequence of computers, there is an opportunity for a hacker and the like to capture information contained in the information packet. Since communication lines comprising the Internet are generally shared by many users, hackers may engage in "sniffing" to capture freely flowing information. Information that

TECHNOLOGY IN THE YEAR 2000 AND BEYOND by Al Harrison

traverses file servers throughout the Internet routinely are saved on backup tapes. Accordingly, confidentiality and security are serious concerns associated with delivering professional services over the Net.

Sending encrypted messages, of course, may be an important precaution for protecting the confidentiality of E-mail messages. Easy to use encryption tools are becoming available for integrating with Web browsers and E-mail applications. Clients should be made aware of the risks involved with E-mail communications and should approve use of E-mail. Encryption software which permits assigning passwords to clients on an individual basis should help demonstrate that reasonable care is being taken to protect client confidences.

Firms should establish Internet E-mail policies and procedures to promote safeguarding client relationships, work product, and to avoid difficulties associated with abuses such as blasphemous language, sexually explicit or implicit language, and other offensive conduct. Firms should consider the merits of reserving the right to review E-mail messages and should reconcile E-mail retention procedures with discovery rules associated with litigation and the like.

While surfing on the Web, practitioners generally encounter on-line database vendors and electronic publishers who strive to generate enthusiasm for their "knowledge bases"; in so doing, such vendors seek to control users' access to the knowledge bases. Based upon the originality of the databases, information vendors may be entitled to copyright in the compilation and presentation of the underlying data. In the course of browsing and downloading information from the Web, practitioners should be aware of the bundle of rights that are associated with the multimedia presentation of information that populates Web sites. In addition to the right to control copying and distribution of the copies, vendors have the right to control access to and use of the information, and to safeguard the integrity of the underlying data. Accordingly, availing themselves of legal counsel, many information vendors now are including Web-wrap licenses on their sites purporting to define the limits of access and use of information obtained from the site. Intellectual property notices (often "buried") particularly on frequented sites should be reviewed for any use limitations.

Representative Meritorious Software:

Adobe Acrobat

FerretSoft InfoFerret Pro, MailFerret Pro, WebFerret Pro

Inso QuickView Plus

Mijenix ZipMagic

Network Associates McAfee Virus Scan, Dr. Solomon's Antivirus, Guard Dog

Qualcomm Eudora Pro

Symantec Norton AntiVirus