

PC Update- Moving Towards the Millennium

Richard G. Kaye, President
MPI Systems, Inc.

ABSTRACT

The Year 2000 problem is in the forefront of today's news with good reason. The potential effects of the problem as it relates to the jewelry industry are significant and will almost certainly contribute to changes in the marketplace. This paper provides a definition and discussion of the problem with specific guidelines for identifying, remediating, and minimizing its impact.

The growth and potential of Intranets, Extranets, and E-Commerce is explored in comparison to current EDI technology. Costs, risks and the potential for competitive advantages are explored, including how it will affect relationships and communication with suppliers and customers.

KEYWORDS

Y2K, Year 2000, E-Commerce, EDI, PCs, Embedded Systems, Jewelry Manufacturing, Software, Minis, PC's, Personal Computer, Mainframe, Remediation, Intranet, Extranet, Internet, Electronic Commerce, Virtual Private Network, VPN, Value Added Network, VAN.

INTRODUCTION

The world is moving towards a globally integrated economy with the Internet erasing international boundaries and facilitating a seamless integration of suppliers and customers. There are no longer any significant technical limitations to direct Internet-based communication of forecasts, orders, shipments, invoices, voice, video, images, technical drawings and any other form of data transmission.

In direct conflict with this, the destructive influence of the Y2K problem seems poised to unravel the structure of existing systems and hurl the unprepared back a few decades to the pencil and paper era.

This paper describes a detailed course of action for the jewelry manufacturer to minimize the effects of the “year 2000” problems from internal and external systems. It also discusses the opportunities coming available to capitalize on E-Commerce as a competitive tool.

THE YEAR 2000 PROBLEM DEFINED

When early systems were developed in the 60's and 70's, disk space and memory were valuable and limited. To save resources, years were stored in terms of two digits. Because of this, many systems will incorrectly interpret the year '00' as 1900 rather than 2000, wreaking havoc on date calculations.

While this seems incredibly shortsighted, most programmers did not expect their applications to last for thirty or more years. Furthermore, many new systems are built upon legacy systems that have this deficiency. Therefore, many modern systems have non-compliant software within their older subsystems.

Some more modern devices contain the similar types of flaws. Some systems were designed to interpret '999' or '9999' as an end of file marker. As a result, a few systems failed on January 1, 1999 due to the '999' in the year. A January 4th article in the Associated Pressⁱ, detailed a few non-crucial but obviously newsworthy failures:

- Taxicab meters in Singapore went dead for about 2 hours on January 1st and could not tally fares.
- Hewlett Packard Defibrillators and another company's patient monitors failed to record the date and time properly until reset.

While basic functions were not affected, this was considered important since over 39,000 defibrillators are in use worldwide.

- Police computers in Swedish Airports went down at midnight Jan 1st when they failed to recognize the year 1999. The problem inconvenienced travelers when they could not issue temporary passports for several hours.

Other dates can have similar effects. For example, many systems do not know that the year 2000 is a leap year. Other dates that will possibly affect systems, for various reasons are:

04-08-1999	09-09-1999	12-31-1999
01-01-2000	02-28-2000	02-29-2000
03-01-2000	12-31-2000	01-01-2001
02-28-2001	12-31-2001	01-01-2002
02-29-2004	12-31-2027	

RELEVANCE TO THE JEWELRY MANUFACTURER

Jewelry manufacturers face multiple threats from the year 2000 issue. To varying degrees, all of the following issues are potential problems:

- Problems with internal systems which prevent or hinder normal operation of your business.
- Suppliers who cannot process your orders.
- Infrastructure failures, such as power outages and telecommunications failures.

For example,

The State of New Mexico will close the state's courtroom for the first week in January, 2000 in order to avoid prob-

lems. The Judicial system's computers are fully compliant but they are dependent upon external systems such as motor vehicle, payroll, electricity and powerⁱⁱ.

- Plant and facility systems failures.
- EDI and E-Commerce failures. This includes third party Value Added Networks (VANs) and Internet Service Providers (ISPs).
- Shipping software problems.
- Customers who cannot place orders or process your invoices.

This potential threat to the continuation of your business requires a definitive course of action.

The jewelry industry is particularly vulnerable for the following reasons:

- *The industry relies heavily upon foreign suppliers.* Many developing countries have no viable plans to address Y2K issues adequately.

98% of all software currently in use in China is piratedⁱⁱⁱ. This includes government and state-owned enterprises. It is therefore unsupported and not legally resolvable.

Similar problems exist in Russia, Thailand, Indonesia, Philippines, and a host of other countries that supply jewelry manufacturers.

See Table 1. The Gartner Group estimates that 66% of companies who are in countries designated as *critical*, will experience at least one mission-critical system failure^{iv}.

Y2K Readiness
Selected countries relevant to the jewelry industry^v

Country	Status	
	Best	→ Worst
Canada	OK	
China	Critical	
Costa Rica	Critical	
Hong Kong	Serious	
India	Serious	
Indonesia	Critical	
Israel	Critical	
Italy	Remediating	
Japan	Serious	
Malaysia	Serious	
Mexico	Remediating	
Philippines	Critical	
Russia	Critical	
Singapore	Remediating	
South Africa	Serious	
Taiwan	Remediating	
Thailand	Critical	
United States	OK	

Table 1.

Legend:

Status is based on the percentage of companies suffering at least one mission-critical system failure:

OK	15%
Remediating	33%
Serious	50%
Critical	66%

The jewelry industry is particularly vulnerable for the following reasons (continued):

- *A preponderance of smaller and often less sophisticated suppliers and customers.* The jewelry industry is composed of many smaller companies who have historically purchased less expensive equipment, such as PC Clones, and may have cobbled together systems based on older software. Smaller companies are also less likely to have professional MIS personnel to manage a remediation program.
- *Dependence upon EDI, as well as other non-standard electronic interchange of data.* Manufacturing jewelers were often forced (for better or worse) into EDI systems by their larger retail customers. Often, this has resulted in primitive PC based stand-alone systems sitting in a corner receiving files that are then re-keyed into non-compliant systems.
- *A large number of custom or in-house developed systems.* Often there is no access to source code or the developer who wrote it and there is little or no documentation. The particular demands of the jewelry industry have made off-the-shelf accounting and manufacturing software almost useless without extensive modifications. Many of the programmers and contractors who performed such work are no longer in business or are no longer employees of the company in which they created the application.
- *Extremely high cost of inventory.* This will prevent or dissuade manufacturers from stockpiling supplies as a hedge against supply interruptions.

WHAT IS AFFECTED?

The scope of the problem is very broad and can be found in both hardware and software. In addition to the obvious mainframe and mini sys-

tems, personal computers can also have problems. Other systems that have embedded computers can also fail.

SUGGESTED STEPS

Larger companies need to follow these steps to avoid problems. Smaller companies may not be able to allocate the same level or resources but will still have to find a way to address the same issues.

1. Project Planning

- 1.1. *Obtain top management support.* The CEO must own the problem. If you cannot get the support you need, seek employment elsewhere and avoid the rush later.
- 1.2. *Formalize responsibilities.* Establish a team of personnel who know the technology. Include HR personnel, facilities engineering and legal counsel. Assess your in house capabilities honestly. If you cannot bring the forces to bear, you should arrange for external support.
- 1.3. *Investigate filing and disclosure requirements.* If your company is publicly held, you may need to talk to legal counsel about SEC filing requirements and Y2K disclosure issues.
- 1.4. *Write a project plan.* Include a schedule with measurable milestones. You cannot control what you cannot measure.
- 1.5. *Set up your remediation record keeping.* You will need to accurately track what is broken and what was fixed both for your own purposes and to document due diligence in the event of a lawsuit.

2. Scoping the project

- 2.1. *Conduct an inventory of all hardware systems.* Include the following: PCs, mainframes, minis, PBX and telephone systems, security access systems, burglar and fire alarm systems, time locks, safes, video surveillance, elevators, escalators, HVAC, point-of-sale and credit card validation systems, burnout ovens, continu-

ous casters and other factory equipment, distribution carousels, sorters, and pick-and-pack systems,

- 2.2. *Conduct an inventory of software as well.* Besides the obvious line-of-business software such as accounting, manufacturing control and order processing systems, include spreadsheets (which may contain 2 year digit calculations), any homegrown applications, such as pricing, tagging, and labeling software, shipping software, programs used for quotes, presentations, adoption sheets, or other sales and marketing tools. Be especially wary of EDI software systems.
- 2.3. *Contact providers of off-the-shelf systems and software.* Determine compliance or availability of patches or upgrades on non-modified systems.
- 2.4. *Contact suppliers of custom systems for compliance information.* If they no longer exist, determine whether the legal successor can provide source code or authorize reverse engineering to recreate the source. When reverse engineering is a possibility, consult your legal counsel first.
- 2.5. *Obtain statements of compliance.* Contact your raw materials, findings, castings and other suppliers to obtain documentation. Where possible, you may want to conduct an on-site audit of critical suppliers to achieve the comfort level you need. Consider lining up alternate suppliers as a backup, especially for foreign suppliers and suppliers who have few competitors.
- 2.6. *Investigate other links in the supply chain.* These may include: brokers, customs agents, shipping companies, etc. Seriously consider replacing vendors now who cannot provide reasonably detailed responses to your request.
- 2.7. *Contact customers.* Verify they have or will have the systems in place to accept your products and process your invoices. If you cannot get paid, little else is of consequence.

3. *Compliance Testing*

- 3.1. The actual testing of systems involves several techniques including testing in an isolated environment. The references section following includes a listing of software tools which may be of help in identifying problems.

4. *Prioritization*

- 4.1. Determine the best method for resolving each non-compliant system.
- 4.2. Call upon the resources at each business functional area within your company to help you prioritize your remediation.

5. *Remediation*

- 5.1. The actual remediation of identified Y2K problems is specific to each situation.
- 5.2. Software patches, upgrades, and replacement are often the obvious solution for systems which are more or less standard off-the-shelf systems.
- 5.3. The first line of defense in resolving custom systems and in-house developed systems is the original developer. If they are unavailable, seek a specialist in this order of preference.
 - 5.3.1. A consultant who specializes in the particular application in question.
 - 5.3.2. A consultant who specializes in the language in which the application is written.

6. *Testing and Validation of Fixes*

- 6.1. Develop a plan to test each application under the direction of a specialist with knowledge of your specific systems. Include powering down and restarting the system after each test date. This typically includes setting up a test environment, developing test

data, aging the data to simulate the test time period, and running the system.

7. *Contingency plan*

- 7.1. As part of your Y2K program, it is imperative to consider external disruptions and how you plan to deal with them. Consider the effects of interrupted service from vendors, utilities, telecommunications, and all of the previously mentioned services you now take for granted.

Y2K CURSE OR OPPORTUNITY?

The author firmly believes that Y2K will not be the end of the world. However, some businesses will fail or falter sooner (as a result of attempting to achieve Y2K compliance) or later (as a result of not achieving compliance). Whenever there is a major shift such as this, opportunities arise for the prepared. Consider the achievement of Y2K compliance as a competitive advantage. It is a means of taking market share from those that are not similarly prepared. The time is now to either accelerate your compliance plan or actively promote your Y2K compliance to your customers.

ELECTRONIC COMMERCE INTRODUCTION

Electronic Commerce ("E-Commerce" or "EC") is defined as the "sharing of business information, maintaining business relationships, and conducting business transactions by means of telecommunications networks."^{vi} This broad definition can be further broken down into three major areas of interest:

- ***Internet Transactions.*** This involves open access and is intended for public use. Most common applications include general information, on line catalogs, and consumer oriented transactions.

- ***Intra-organizational transactions (Intranets)***. This involves communications, internal to the company but not necessarily within one location or site. Access is private and proprietary. An example of this might be to provide field sales people with up-to-the-minute order and inventory information via a link to the home office.
- ***Extra-organizational transactions (Extranets)***. This involves communication to another business entity, such as between supplier and customer. Access is controlled and involves selective sharing of information on sales, order status, sell-through, inventory positions, etc.

BACKGROUND

During the 1980's, EDI emerged as the *de facto* standard for interchange of data between customer and supplier. It has achieved tremendous market penetration due in part, to the fact that the sender and receiver of the data were platform independent. EDI is now in use by close to 100,000 companies in the US who together conduct about \$130 billion in annual sales. Currently, the most prevalent means of handling EDI transfers is through Value Added Networks (VANs). VANs are third party providers who accept inputs from the sender and batch forward the data to the recipient.

Most retailers have embraced EDI as part of their standard business operating systems. Wal-Mart processes in excess of 100,000 EDI transactions per day with over 5,000 partners. Service Merchandise began EDI in 1986 with a large VAN, Sterling Commerce. They now have over 700 trading partners using EDI.

INTERNET TRANSACTIONS

Most jewelry companies already have web sites and email capability. The cost of entry into this technology is extremely low. The Manufacturing Jewelers and Suppliers Association (MJSA) offers no-charge web sites to all members and enhanced web site setup and design at a modest cost.

However, since the Internet is an open and essentially insecure environment it is inappropriate intra-company or inter-company transactions.

INTRANETS

Intranets may be thought of as forms-based email with web pages, video, file transfer and images. This is currently a very hot market because it greatly facilitates dispersion of organizational information such as manuals, catalogs, and technical documents while offering levels of security. Furthermore it enables physically separate groups within the organization to collaborate on projects such as product design, catalog development and quote preparation.

Off-the-shelf hardware^{vii} and software from Microsoft® (Windows NT Server and Proxy Server) and others makes it relatively simple to set up Virtual Private Networks (VPNs). This technology utilizes Internet access to create a secure “tunnel” into the home server thereby bypassing most telephone charges. The outside sales person or branch office connects to a local Internet Service Provider (ISP) to establish the connection. From this point on all data transmissions occur in a secure environment.

VPNs can offer substantial savings over leased lines or 800 number dialup. A recent comparison of costs conducted by PC Week Online^{viii} cited different costs and pricing schemes such as a flat around \$25 per month per user or \$2.50 per hour of connect time.

EXTRANETS

The development of the Intranet will often lead one to look for the same types of advantages in communication with suppliers and vendors. While still not widely adopted, Extranets will undoubtedly be the most widely used form of business-to-business transaction processing, probably within 5 years. While EDI promised to bring these benefits to all users, the cost

and complexity of VAN-based EDI has prevented more widespread use. The promise of the Extranet is its lower cost of entry and ongoing costs.

Traditional EDI companies such as Harbinger/Premenos and Sterling now offer Internet based EDI software as an alternative.

Non-EDI Extranet solutions are being used as an intermediate step. The Army-Air Force Exchange Service (AAFES), the \$7 billion retailer, is a significant presence in jewelry retail. AAFES offers non-EDI suppliers the opportunity to view invoices, and to send and receive shipment orders and information. JC Penny offers similar information on its own web-based system.

BENEFITS OF AN EXTRANET

Through use of the Internet, companies stand to benefit from reduced transmission cost and near instantaneous transmission of data. They also can achieve greater flexibility in integrating their own applications with the creation of Internet-based communications to their suppliers and customers.

MAIN CONCERN - SECURITY

Security is the primary concern in any Internet based transaction processing system. This can be addressed in terms of the following four issues:

- ***Confidentiality.*** Transmissions are only available to the designated recipient.
- ***Integrity.*** The entire transmission arrives verifiably intact.
- ***Authentication.*** The sender can be verified.

- *Non-repudiation of origin and receipt.* The sender can be assured that the recipient received the transmission and the receiver can be sure of the origin of the document.

Various encryption and authentication technologies are available today which have demonstrated high levels of security. CommerceNet^{ix}, a trade organization, has promoted standards for security such as, S/MIME and EDI-INT, have been adopted by leading providers of Internet based E-Commerce.

COST FACTORS

VAN charges to transfer data, are typically based on a set rate per kilo-character of data transmitted, plus numerous other fees. A medium volume EDI program of 200 to 2,000 documents per month, costs from \$2,788 to \$6,530 for the first year, versus \$412 to \$758 over the Internet^x.

VANs provide additional services however, such as providing an audit trail for missing transmissions, startup assistance, and technical support. Therefore, a direct comparison of costs are not as significant.

CONCLUSION

Intranets, Extranets, and E-Commerce are natural extensions of the convergence of Internet and EDI technologies. They provide the means for reducing the cost of doing business by streamlining the customer and supplier interfaces while providing automation tools for distribution of intra-company information.

While this technology is relatively new, it has nonetheless matured to a point that most companies should investigate its potential in terms of their own costs and needs. The cost of implementing leading edge technology such as this, can involve a substantial learning curve. However, the author believes the competitive advantages are so significant that those

who are currently using EDI need to make plans to move into this new technology, as soon as practical.

APPENDIX

Where to get more information about Y2K

- www.nrf.com The National Retail Federation. Includes important information about the Y2K readiness of various suppliers and vendors.
- www.year2000.com Consultant Peter de Jager's site.
- www.itaa.org The Information Technology Association of America.
- www.sba.gov/y2k The Small Business Administration's Y2K page.
- www.nist.gov/y2k The National Institute of Standards and Technology
- www.boma.org/year2000/ The Building Owners and Managers Association.
- www.y2k.gov The President's Council on Year 2000 Conversion.
- www.itpolicy.gsa.gov – The General Services Administration.
- www.sec.gov The Securities and Exchange Commission.

Software to help with Y2K Problems^{xi}

- **Assessment/inventory tools /code searchers**
 MicroFocus Revolve 2000
 Systemvision 2000
 Viasoft Existing System Workbench
 Survey 2000 from Prince Software
- **Code remediators/changers**
 Translate 2000 from Prince Software

- **Date simulation tools**
 Compuware's XPEDITER/Xchange
 HourGlass/2000 (also available for client/server)
 Time Machine (also available for client/server)
 Simulate 2000 from Prince Software
 Viasoft Validate
 Compuware's File-AID/Data Ager
- **Change control tools**
 Princeton Softech's Version Merger
 CA-Endevor
- **Recorder/playback for CICS tools**
 Compuware's QA Hiperstation
 Mercury interactive
 Technology Builders Inc.'s Test Director
 Technology Builders Inc.'s Winrunner 2000
 Technology Builders Inc.'s Loadrunner
 Logic Works' Testbytes
 Autotester

Website Info on E-Commerce

<http://www.brint.com/Intranets.htm> BizTech network's Intranet page

<http://www.brint.com/Elecomm.htm> BizTech network's E-Commerce page.

<http://www.zdnet.com/pcweek/sr/ecommerce/main.html> PCWeek Magazine on line page about E-commerce

<http://www.ecommerce.gov/emerging.htm> United States Dept of Commerce report on E-Commerce. See Appendix 3 "Electronic Commerce between Businesses: Analysis and Case Studies.

<http://www.fortresstech.com> Fortress Technology

<http://tlogic.com> Technologic Products
<http://www.Sterlingcommerce.com> Sterling Commerce
<http://www.harbinger.com> Harbinger Premenos
<http://www.commercenet.com> Commerce Net
<http://microsoft.com.directaccess/feature/99/0127.htm> Microsoft
Direct Access: Proxy Server and Virtual Private Networks

ⁱ Chris Allbritton, *Early Glitches Appear Unfounded*, January 04, 1998 17:10 EST, Associated Press

ⁱⁱ Stephanie Neil, *The Court Adjourns for Y2K*, January 25, 1998 PC Week

ⁱⁱⁱ US Embassy in Beijing report, February/May 1998 as reported in "A Global Guide to Y2K" by Eric Helwig, *Business 2.0* January 1999

^{iv} Source US Embassy in Beijing report dated February/May 1998 as reported in "A Global Guide to Y2K" by Eric Helwig, *Business 2.0* magazine January 1999.

^v Gartner Group, "Year 2000 Global State of Readiness and Risks to the General Business Community" October 1998 as reported in "A Global Guide to Y2K" by Eric Helwig, *Business 2.0* magazine January 1999

^{vi} Vladimir Zwass, 1996 "Electronic Commerce: Structures and Issues", *International Journal of Electronic Commerce*

^{vii} two vendors of VPN Hardware are: FortressTech at <http://www.fortresstech.com> and Technologic Products at <http://tlogic.com>

^{viii} Pankaj Chowdhry, *VPNs Save Time and Money—Sometimes*, August 22, 1998

^{ix} CommerceNet can be reached at <http://www.commercenet.com>

^x Don Dugdale, *Business Does Business Over the Internet* September, 1996 as reprinted in <http://www.uniforum.org/news/html/publications/Sept96/internet.html>

^{xi} The author makes no representation as to the effectiveness or overall suitability of any products listed. The presence or absence of any product in this listing should not be construed as an endorsement or negative indication.

