Year 2000: Business and Legal Ramifications

BY GERHARD ADAM

Failing to achieve Year 2000 compliance can have a far-reaching impact not only the IT organization, but on those individuals it employs, including the technicians. While most technicians view this problem as just another project, they remain largely uninformed of the full range of legal consequences.

This article discusses some of the serious non-technical consequences of failing to achieve Year 2000 compliance. While many technicians view this problem as just another "project," they remain largely uninformed of the full range of effects that may result from non-compliance. Much of the information in this article was obtained from legal papers available on the Internet, as well as discussions with attendees of various technical conferences.

It is incumbent upon the technician to appreciate that the Year 2000 (Y2K) problem extends far beyond the boundaries of the IT organization and is a business problem, not a technical one.

Let me start by saying that this article is not simply "fear-mongering," which is a common charge leveled by technicians whenever such consequences are discussed. It is incumbent upon the technician to appreciate that the Year 2000 (Y2K) problem extends far beyond the boundaries of the IT organization and is a business problem, not a technical one. This shift in perspective means that any problems encountered as a result of failing to achieve Y2K compliance may cause the entire business,Y2K project, and IT processes to be reviewed by non-technicians (i.e., shareholders, lawyers, and judges). If decisions made regarding Y2K compliance are not defensible in this context, then serious issues of liability will occur.

This article is not intended to meticulously address legal details, but rather to raise issues which need to be examined in each organization by those who have legal and fiduciary responsibilities to the corporation. The role of the technician in ensuring that the appropriate information is provided may determine the extent to which liability exists.

It has been suggested by some technicians that to raise these issues may jeopardize their careers. Whether such a position is accurate, it is highly unlikely that anyone's job would be threatened by raising legitimate, well thought out concerns (as opposed to turning it into a personal crusade). The most immediate concern, however, should be whether your own actions (or lack thereof) could result in consequences far beyond the loss of a job. Additionally, technicians should appreciate the fact that regardless of the technical reasons for Y2K decisions, the results must be defensible from a legal perspective. It matters little what technical approach is used to solve the problem; however, failure may matter a great deal when scrutinized in a court of law.

BACKGROUND

Historically, most systems development project issues of liability and legality have been typically assumed by end-user departments. These departments have established the requirements and are responsible for ensuring that the results are consistent with the objectives of management as well as the laws to which they may have been subject. The Y2K is unique in that its requirements have not been established externally, but rather as a consequences of technical decisions made over several years. This has resulted in a situation where the IT organization bears singular responsibility for the functioning of the business systems, depending largely on the degree to which management and the end-user community have been kept informed. In many corporations, the IT organization has not been proactive in raising awareness of the Y2K problem and, consequently, may incur the greatest liability for this failure to disclose this information.

LAWS (MANAGEMENT)

One of the legal issues affects the executive officers and directors of corporations. The SEC Securities Act Release No. 6385 requires full disclosure regarding impacts known and/or anticipated with respect to the operation of the business. This duty exists when an "uncertainty is both presently known to management and is reasonably likely to have material effects on the registrant's financial condition or results of operations." This act makes management liable for material misstatements and omissions to any person acquiring stock.

In most cases, the duty of the directors is variously identified as being exercised in "good faith" and in a manner consistent with that of an ordinarily "prudent person in a like position" and similar circumstances. In addition, there is a responsibility to exercise "due diligence" in the pursuit of achieving compliance which extends beyond simple rhetoric.

In addition, this places the IT organization in a pivotal position regarding the flow of information regarding Y2K compliance. If the information presented by the IT organization to its management is misleading or untrue, it is entirely possible that liability would shift and may result in criminal enforcement actions.

LAWS (TECHNICAL)

Of consequence to the technician is an understanding of computer crime legislation and its sometimes vague definitions. For example, a person is guilty of the computer crime of interruption of computer services when he, without authorization,intentionally or recklessly disrupts, degrades or causes the disruption or degradation of computer services, or denies or causes the denial of computer services to an authorized user of computer systems.

Similarly, statements within the law state that a crime has occurred if a person "intentionally or recklessly and without authorization ... damages, destroys, or takes data intended for use by a computer system ... " What should be of concern to technicians is that these laws clearly allow a great deal of freedom regarding interpretation of these acts. While it seems intuitively obvious (to the technician) what is being described, this same law could be used in a variety of enforcement actions.

While there is still controversy surrounding many of the "alarms" being raised, it is important to remember that in approximately 2.5 years the various opinions will be either validated or discarded.

SCENARIO

Let's suppose that a company fails to achieve Y2K compliance and suffers multi-million dollar losses as a result. The shareholders (and potentially affected customers) litigate for damages. One of the first things that will be examined is whether the executive officers and dire tors acted in a prudent and reasonable manner in protecting the assets of the corporation. However, let's further assume that upper management has documented and taken "reasonable" steps to resolve the Y2K problem. So the possibility exists that blame may start to shift further down the line. In many cases it may stop at the CIO or IT director level, but let's consider other possible implications as well.

For a variety of reasons, let's assume that the approach for resolving the Y2K involved some technical choices and allocation of resources which proved to be inadequate. As a result, some of the techniques employed didn't work properly, testing was insufficient, and the system failed to perform as expected.

If we apply the interpretation of computer crime laws to this scenario, what are the possible interpretations?

- Who granted authorization for the work to be performed in that manner?
- Would outside experts agree with your choices and decisions?
- Were the decisions made, intentional, considering all the consequences?

It should be relatively easy to see, that the Y2K project fails there will be arguments, mostly occurring from 20/20 hindsight. However, the ability to defend against an "expert" witness who refutes your approach, upper management claiming that they never granted authorization for that particular technique, or interpretation that testing and implementation were undertaken in a "reckless" manner, could result in the technical defendants being accused of a crime.

While it is not my intent to represent legal advice, it is important that technicians understand that their actions may have serious consequences for the organization (and themselves) far beyond the scope of anything they've ever encountered. Even if the scenario presented is unlikely, it would almost certainly result in the termination of individuals implicated in such a failed project.

The central issue is for IT organizations to begin behaving as if their actions were being scrutinized by the legal system. The need to create a "paper trail" cannot be overstated. If there is the slightest possibility that a choice or approach may be indefensible in the future, the need to document activities becomes critical.

DEFENSE

To defend yourself properly, there are some basic elements which must exist to satisfy the law:

1. Proof that the problem was taken seriously and acted upon. This could include the establishment of a project management team, subscriptions to Y2K publications,Y2K seminars, etc.

2. Hardware/software inventory should exist to indicate that an effort was made to determine all "at risk" applications.

3. Impact analysis or risk assessment to evaluate the organizational impact.

4. Proactive communication throughout the organization to raise awareness and address impacts and solutions.

5. Project plan, budget, staffing, etc., (i.e., basic resources have been allocated to address the problem).

In short, you must make a serious attempt at resolving the Y2K problem and be prepared to document the entire process.

SOUND THE ALARM

This article should help you begin the process of alerting individuals that the risks associated with the Y2K extend far beyond simply being another IT project. The individuals within an organization who share some of this responsibility should be made aware and be utilized to raise awareness. Some of these individuals will be internal legal staff and auditors. Both groups should be contacted by IT organizations (if they haven't been already), and presentations and seminars should be conducted for end users regarding the consequences of the Y2K. While there is still controversy surrounding many of the "alarms" being raised, it is important to remember that in approximately 2.5 years the various opinions will be either validated or discarded. The only question which remains is whether your opinion is defensible should the need arise. *ts*

Gerhard Adam, president of SYSPRO, Inc., has 23 years of experience in large systems computing, specializing in performance and MVS/ESA internals. He has been involved in development that extends from access method interfaces and telecommunications to AFP software.