operations. There is a problem with the old equipment.

A great deal of our security programs interact with hardware date and time, and security administrators should verify that all hardware will be able to make the transition smoothly. One alternative at this stage is to advance the clock on the system and see what transpires as the computer moves into the 21st century. This is no great problem with most stand-alone equipment but there are many systems with which we cannot take the risk of crashing.

For the PC user there are two freeware programs which will test a computer's ability to enter into the year 2000. The first program, *DOSCHK.EXE*, tests the behavior of a microcomputer operating under DOS or Windows95. It simulates the last 10 seconds of the century and checks the DOS, BIOS and CMOS dates.

A companion program, *Year2000*, is a memory resident program which will help adjust the date of a recalcitrant microcomputer when the millennium arrives.

Both programs in Zip format are available from the web site: http://www.RighTime.com, but test at your own risk. The site incidentally has several other programs you might find of interest.

PROBLEMS AND SOLUTIONS — Q: and A:

Over the years we have received letters, telephone calls, fax and electronic mail from individuals about information security products as well as security-related and computer problems. And we assisted them. We would like to extend that service to all readers who have heretofore not availed themselves of our assistance. You can reach us at:

- **Postal address:** Dr. Harold Joseph Highland, Computers & Security, 562 Croydon Road, Elmont, NY 11003-2814, USA
- **Electronic mail:** Highland@dockmaster.ncsc.mil as *primary mbx* and *backup* [if needed] to hjhighland@juno.com
- **Telephone:** [+1] 516.488.6868
- **Fax:** Number and conditions available upon request.

Virus Scanners for Multiple OSes

During the last several months we have received inquiries about the possible need to use more than one antivirus product on microcomputers using multiple operating systems. Some have micros running Windows 3.11 and Windows'95, others with Windows'95 and Windows NT, a few with Windows NT and OS/2, several with Windows'95 and Linux. Others have microcomputers capable of running three operating systems. I, and some of my friends at other publications, are using microcomputers with four or more operating systems.

There seems to be some confusion among readers; a few are following procedures that make their systems open to virus attack. There also seems to be some misunderstanding about the license agreement made with antivirus producers.

A single recommendation cannot be made because of the multiple complexities of the microcomputers.[1] Combining disparate file systems such as FAT16, FAT32, OS/2, NT, Linux, or Unix file systems on the same hard drive, requires the proper product for the respective platform. If the microcomputer, for example, has NTFS or HPFS file systems and is booted from a DOS diskette, the DOS scanner will not be able to access the files on those file systems. Similarly, a Windows'95-only scanner would be insufficient, because if the machine's boot sector becomes infected, one would have to boot with a clean, protected DOS disk and run the DOS scanner in disinfection mode.

[1] To assure our providing readers with the most accurate information, we asked several anti-virus technicians whom we felt were best able to resolve this problem for their views. We therefore would like to thank David M. Chess, a Research Staff Member at IBM's Watson Research Center, and a member of the IBM AntiVirus R&D team; Vesselin Bontchev, anti-virus researcher, of FRISK Software International; Shane Coursen, Senior Technology Consultant at Dr Solomon's Software in the States; and Sarah Gordon, an AntiVirusResearch Consultant at the IBM TJ Watson Research Center.

In general it is not a good idea to try to use an antivirus product intended for one platform to protect a different platform. If all drives are accessible through DOS, for example, it would be possible to scan those drives simply using a DOS command line scanner. The long filename files under Windows'95, for example, are not readable by a scanner for Windows 3.1. Also if one tries to maintain active protection against viruses, including the macro variety, it would be best to provide that protection for each operating system.

The cost of *extra* antivirus protection in a business environment is generally nil. Please note that this is *not* true of the antivirus packages sold to individuals at retail. Most vendors provide protection *by machine*, and if it uses more than one operating system, the added protection is provided. This is done by one of two ways:

[1] some antivirus software producers package their product so that multiple operating systems can be protected by the various versions on their disk(s). For example, the IBM AntiVirus Desktop Edition includes support for DOS and Windows 3.x and Windows 95 and OS/2. Their Enterprise Edition also includes support for NT and Novell NLM.

[2] some antivirus software producers have a corporate license, such as Dr Solomon's, that protects the workstation regardless of the number of operating systems running on it. In my own case I receive updates for DOS, Windows 3.x, Windows'95, Windows NT, OS/2 and Novell.

Recommendations: In a corporate environment it is best to protect each OS with its own antivirus program. It is also best to maintain an active scan, checking each program and document [if necessary] as it is loaded and/or copied. Updating each OS program takes time, but it takes far less time than cleaning a system which has been infected by a virus.

Changing Passwords

How often do you require users to change their passwords? Why? Tradition in the company? Industry practice?

In the E-mail world I belong to a private small chat group. Actually it consists of a group of individuals with a common interest in computers, security and technology, which over the years has become a social group as well. If anyone of us has a problem, just put it on the board and see what help [or hell] one might get. One such question came from the eastern part of Europe.

"What is the reasonable time for an ordinary user to change a password?"

Forgetting for the moment the definition of *ordinary*, here are some factors that should be considered when determining the 'life time' of a password:

- Sensitivity of the data.
- Computer-sophistication of the user.
- Quality of the password.
- The operating system used.
- Burden on the security director.
- Level of risk of an attack.
- Status of channel security.

The lifetime of a password depends upon the environment. Few with home computers use passwords. One of our group uses the same password indefinitely. I use a password under Windows NT and change it periodically or after a serviceman has tuned it up.

In many offices which require a password change every month, the level of security is nil since passwords, unless verified for robustness, are easily guessed. Chances are one needs little training in breaking into systems to attack these. A while back I helped a local company to instal a password saver on the system. After four months I found the lead documentation writer was creative with passwords: Jan1997x, Feb1997x, Mar1997x, Apr1997x. Most others were in the same class. These are experience programmers in a software development company.

Most experts agree that the more sensitive the information, the more frequent the change of a password. But this works only if password selection is properly administered. To improve security at the local soft-

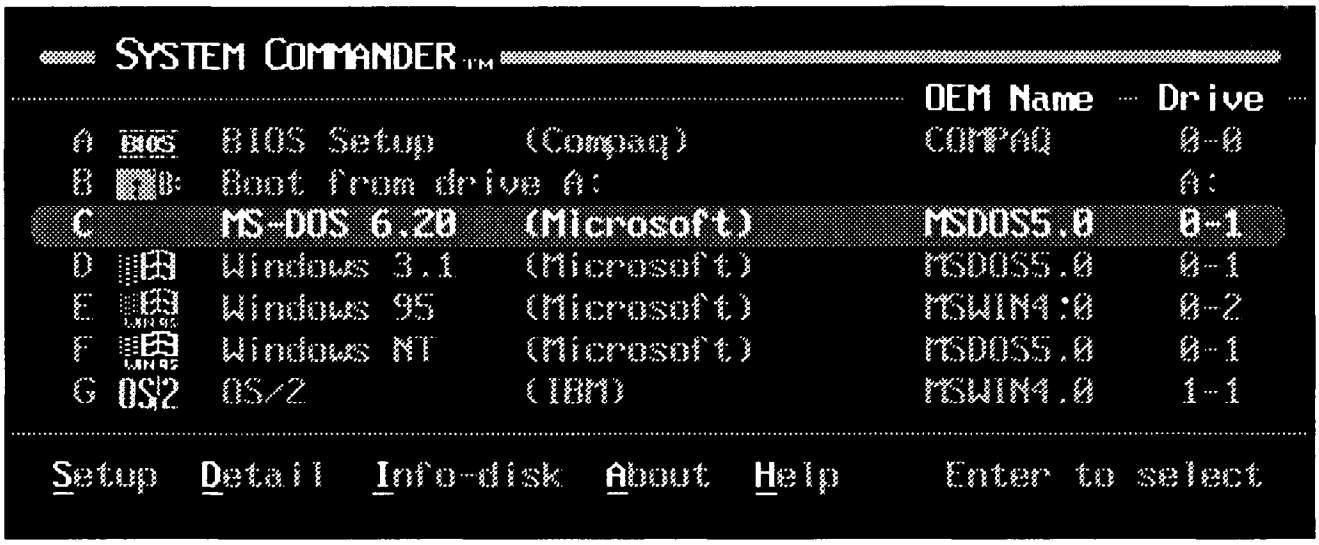

Fig. 1.

ware house, the management introduced several changes.

- All passwords had to be eight characters long.
- Each had to include alphabetic and number characters, a minimum of two of each.
- Most passwords [clerical staff and low level coders] were changed every 36 to 37 days.
- A log was maintained and any password could not be re-used in less than 13 months.
- Those handling most sensitive data had to use both a password and a token.
- All passwords were screened by a list that included a standard dictionary to which all employee names, street names, town names, family names [wife, children, parents and siblings] were added. Also included were local street and store names as well as a number of computer terms. As the system has been working, the company added a number of foreign words which they found employees using.

Before you concern yourself with frequency of password change, institute a password control policy. Frequently changed passwords, that are poor, lead to a sense of false security.

Why I bought a Compaq

In the past each time I announced a new test machine, I invariably had several readers query me about my choice of configuration and brand. Early this year my new computer arrived. I had upgraded my test computer to a Compaq 200 MHz Pentium Pro with 64 Mb of EDO RAM and an L2 256Kb pipeline burst external cache. Since I test products under different operating systems I use System Commander[2] so that I am able to boot directly into various operating systems, specifically: MS-DOS 6.2, Windows 3.1, Windows'95, Windows NT and OS/2 [see *Fig 1.*]

Why did I buy another Compaq? I could provide considerable technical evidence for selecting the specific system with a Matrox MGA Millennium graphics accelerator card with 4Mb on board, a Universal Serial Bus and a SCSI card; furthermore it is energy efficient. I selected a Deskpro 2000 since I already had my network boards and saw no reason to pay extra for a 4000 or 6000 machine with features I did not currently need. Instead I had two additional

[2] *System Commander* is a product of V Communications, 4320 Stevens Creek Blvd, Suite 120, San Jose, CA 95129. phone 408.296.4224; fax: 408. 296. 4441.