WATCHDOG®

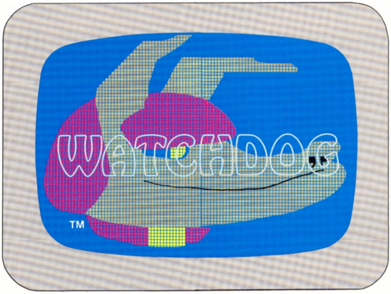
Gahan Wilson
WORLD'S NUMBER ONE COMPUTER SECURITY PROTECTION
WATCHDOG'S FIRST ASSIGNMENT
WATCHDOG
ALL SYSTEMS PROTECTED
WATCHDOG OF CORPORATE COMPUTER SECURITY

PC
Data Security

FI™ FISCHER INNIS SYSTEMS CORPORATION

The **Watchdog** PC data security system provides:

- ID and password control to prevent unauthorized access.
- A security administration option to allow or require users to periodically change their own passwords.
- Permissions that govern the scope of user activities, such as whether a user may read files, write to files, create and delete files, or use the DOS commands.
- Integrated access control and automatic data encryption, which is transparent to authorized users, for the strongest security available.
- Directory-by-directory protection that allows control over which users may access particular directories.
- Protection against unauthorized attempts to access hard-disk data.
- Protection against accidental or malicious formatting of the fixed disk.
- Audit trail to record user activity by user ID, project ID, directory accessed, program executed, date, and time.
- Audit trail records system use and security violations for review on-screen or in printed reports.
- Audit trail report formats may be saved as report sets and reused as necessary.
- System library for efficient storage of programs that are used from more than one area (directory).
- Area Menus to give convenient selection of directories and programs.
- Help screens for on-the-spot user guidance.
- Electronic Mailbox facility to send messages between system users.



Watchdog *is a better buy.*
PC Products, March 1985

Watchdog *is designed with today's complex software in mind....*

A sophisticated, comprehensive package that takes security very seriously.
Lotus, October 1985

Watchdog *provides an efficient security system...that is not encumbersome or bothersome to use.*
Datapro Report on Information Security, October 1985

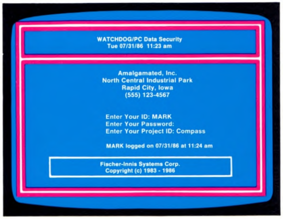
Watchdog is the PC data security system of choice at major corporations, medium and small sized businesses, Government agencies, and the Armed Forces. Fischer-Innis Systems Corporation, one of America's foremost developers and marketers of software products for IBM mainframe computers, stands behind *Watchdog*'s success.

Fischer-Innis Systems Corporation's commitment to product support is unsurpassed in the industry. Our Customer Support Group will respond quickly to your questions and will provide whatever level of assistance you require. Additional ongoing maintenance plans are available. Such plans allow us to establish and maintain close relationships between our company and the individual and corporate users of our software products.

You've invested in a high-quality PC . . . Now invest in a high-quality data security system.

Watchdog is the data security system for your PC. Access control, data encryption, separate levels of permissions, and audit trails are integrated in one easy-to-use package to provide the most effective security software for protecting data on your hard disk.

The same features that make PCs flexible and easy-to-use also make the important data they store vulnerable to theft and misuse. *Watchdog* ensures control and protection, while allowing you to maintain the versatility and power of the PC.



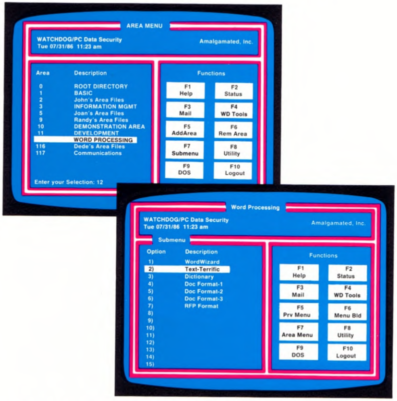
```
WATCHDOG/PC Data Security
Tue 07/31/86  11:23 am

Amalgamated, Inc.
North Central Industrial Park
Rapid City, Iowa
(555) 123-4567

Enter Your ID: MARK
Enter Your Password:
Enter Your Project ID: Compass

MARK logged on 07/31/86 at 11:24 am

Fischer-Innis Systems Corp.
Copyright (c) 1983 - 1986
```

ACCESS CONTROL *Watchdog*'s first line of defense is access control. To log on to the PC, you must enter a personal user ID and password. Without these, *Watchdog* denies access to all programs and files stored in protected directories. You may also be required to enter a project ID.

As a security administration option, users may be allowed or required to periodically change their own passwords. Frequently changing passwords can enhance system security.

Watchdog also guards against improper attempts to access data on a hard disk by: preventing boot-up with DOS on a floppy diskette to access the hard disk; interrupting the boot-up of the hard disk; or employing utility programs designed to access hard-disk data.

FORMAT CONTROL With *Watchdog*, you can control the use of the FORMAT command. Concern about destruction of data by accidental or malicious formatting is eliminated.



```
AREA MENU
WATCHDOG/PC Data Security                    Amalgamated, Inc.
Tue 07/31/86  11:23 am

Area    Description                          Functions
 0      ROOT DIRECTORY                  F1 Help       F2 Status
 1      BASIC                           F3 Mail       F4 WD Tools
 2      John's Area Files               F5 AddArea    F6 Rem Area
 3      INFORMATION MGMT                F7 Submenu    F8 Utility
 5      Joan's Area Files               F9 DOS        F10 Logout
 9      Randy's Area Files
10      DEMONSTRATION AREA
11      DEVELOPMENT
        WORD PROCESSING
116     Dede's Area Files
117     Communications

Enter your Selection: 12
```

```
Word Processing
WATCHDOG/PC Data Security                    Amalgamated, Inc.
Tue 07/31/86  11:23 am
Submenu
Option    Description                        Functions
 1)       WordWizard                    F1 Help       F2 Status
 2)       Text-Terrific                 F3 Mail       F4 WD Tools
 3)       Dictionary                    F5 Prv Menu   F6 Menu Bld
 4)       Doc Format-1                  F7 Area Menu  F8 Utility
 5)       Doc Format-2                  F9 DOS        F10 Logout
 6)       Doc Format-3
 7)       RFP Format
 8)
 9)
10)
11)
12)
13)
14)
15)
```

AREA MENU SYSTEM In *Watchdog*, protected DOS directories are referred to as "areas." Up to 256 areas may be listed on full-screen menus for convenient selection. The menus help you organize and manage your information, as well as protect it. A common approach to area assignment is to give each user one or more personal areas for securing their private files. Then, additional areas may be designated for files and programs that are to be shared among groups of users, for example, word processing, spreadsheet, or data base management programs.

Access to each area is controlled. *Watchdog* will allow you into an area, but only after first checking your authorization.

For each area selection on the menu, you may create submenus to list programs, subdirectories, or batch files in that area. Programs selected from submenus will begin executing automatically, if you wish. Submenus may be nested, with no limit on the number you may create for each area.

Once you are permitted into an area, a submenu displays selections for each program in that area. *Watchdog* continuously monitors all movement on the PC from the point of log-on, and will not allow you to move from one area to another without first checking your authorization. You may access multiple areas simultaneously to facilitate copying information between areas, or to allow you to use the concurrent processing offered by multitasking packages.

As an alternative to working from the menu system, applications may be seamlessly embedded into *Watchdog* so that they begin executing as soon as the user logs on.

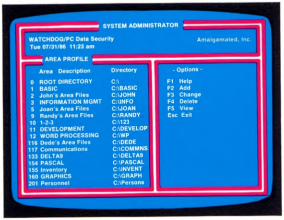
PERMISSIONS Multiple levels of permissions strengthen *Watchdog*'s security, at the same time making *Watchdog* protection more flexible. Permissions are options that you select to determine the "span of control" users will have when working with the system. Permissions are set on three levels: for the system as a whole, for each area (DOS directory), and individually for each user.

System permissions regulate systemwide conditions, such as whether users may edit the AUTOEXEC.BAT file or the CONFIG.SYS file, or whether users will be automatically logged off the PC after a specified inactive period.

Area permissions and User permissions work in combination to determine the kinds of activities a particular user may perform in a given directory. *Watchdog*'s flexible system of permissions lets you establish customized protection for your particular needs. Profiles, which are set up for each user and each area, allow *Watchdog* to cross-reference your ID and password with the permissions you have in the areas you may access. *Watchdog* checks profiles each time you select an area, and allows only those operations permitted to *you* in *that area*.

For example, you might store spreadsheet templates in a "read-only" directory so that users may access them but may not modify them. Or, you might designate that the permissions associated with data entry files (such as personnel files or payroll files) be determined not only by the directory in which they are stored, but by which user is accessing them. This way, clerks may add new information to existing files, but may not read, create, or delete files. The manager may, on the other hand, read and write to files, as well as create and delete files.

For added protection, permissions also govern whether users may have access to the DOS commands from within a specific directory.



```
                    SYSTEM ADMINISTRATOR
WATCHDOG/PC Data Security                    Amalgamated, Inc.
Tue 07/31/86  11:23 am

AREA PROFILE
   Area  Description          Directory          - Options -

 0   ROOT DIRECTORY          C:\               F1  Help
 1   BASIC                   C:\BASIC          F2  Add
 2   John's Area Files       C:\JOHN           F3  Change
 3   INFORMATION MGMT        C:\INFO           F4  Delete
 5   Joan's Area Files       C:\JOAN           F5  View
 9   Randy's Area Files      C:\RANDY          Esc Exit
10   1-2-3                   C:\123
11   DEVELOPMENT             C:\DEVELOP
12   WORD PROCESSING         C:\WP
116  Dede's Area Files       C:\DEDE
117  Communications          C:\COMMNS
133  DELTA9                  C:\DELTA9
154  PASCAL                  C:\PASCAL
155  Inventory               C:\INVENT
160  GRAPHICS                C:\GRAPH
201  Personnel               C:\Persons
```

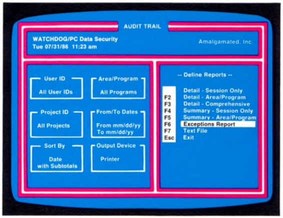
AUTOMATIC DATA ENCRYPTION *Watchdog*'s data encryption provides the highest level of security available. With encryption, the protection is built into the data itself. Keys are set up once by the System Administrator and are totally transparent to users. Users do not have to memorize, record, or enter keys to encrypt or decrypt data files.

Watchdog uses a proprietary encryption algorithm. The U.S. Department of State has made *Watchdog* subject to the same export control restrictions as DES (the Data Encryption Standard algorithm).

When encryption is active for an area, all programs and files will reside on the disk in encrypted form until retrieved by an authorized user. Once selected, a program or file is automatically unscrambled and presented in plaintext form. When work is completed, the data is automatically returned to a scrambled form for protection. This ensures security because you cannot neglect to encrypt the data. Data is protected by default.

Encryption and decryption are transparent. They are performed in the background, and are so fast that there is no noticeable slowdown in response time.

The System Administrator can selectively activate the encryption feature in each area on the system by specifying an encryption key.



AUDIT TRAIL

WATCHDOG/PC Data Security
Tue 07/31/86 11:23 am

Amalgamated, Inc.

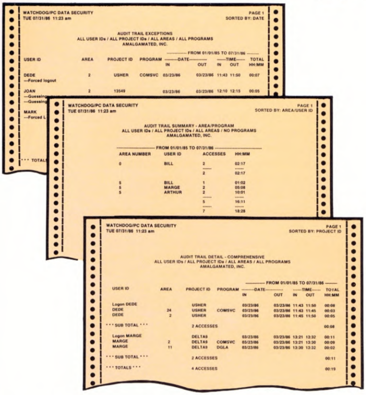
User ID: All User IDs
Area/Program: All Programs
Project ID: All Projects
From/To Dates: From mm/dd/yy To mm/dd/yy
Sort By: Date with Subtotals
Output Device: Printer

-- Define Reports --

Detail - Session Only
F2 Detail - Area/Program
F3 Detail - Comprehensive
F4 Summary - Session Only
F5 Summary - Area/Program
F6 Exceptions Report
F7 Text File
Esc Exit

AUDIT TRAILS *Watchdog* records an audit trail to monitor system use. Detail, summary, or work-session information may be reviewed on-screen, or in printed form. Over 100 formats are available for customized reporting.

You may sort audit trail data by user ID, area, date and time, program executed, and project ID. Details of sensitive system activity (such as use of *Watchdog*'s encrypted backup and restore utilities), and of security violations (such as attempts to illegally change from one directory to another) are also recorded by the audit trail. A complete history file can be processed with a data base manager or report generator to prepare custom reports.



```
WATCHDOG/PC DATA SECURITY                                                        PAGE 1
TUE 07/31/86  11:23 am                                                 SORTED BY: DATE

                              AUDIT TRAIL EXCEPTIONS
              ALL USER IDs / ALL PROJECT IDs / ALL AREAS / ALL PROGRAMS
                                 AMALGAMATED, INC.

                                          ----------- FROM 01/01/85 TO 07/31/86 -------
USER ID          AREA   PROJECT ID   PROGRAM  --------DATE---------   -----TIME-----  TOTAL
                                              IN            OUT       IN     OUT      HH:MM

DEDE               2      USHER      COMSVC   03/23/86      03/23/86  11:43  11:50    00:07
---Forced logout

JOAN               2      13549               03/23/86      03/23/86  12:10  12:15    00:05
---Guessing
---Guessing

MARK
---Forced L

*** TOTAL
```

```
WATCHDOG/PC DATA SECURITY                                                        PAGE 1
TUE 07/31/86  11:23 am                                         SORTED BY: AREA/USER ID

                       AUDIT TRAIL SUMMARY - AREA/PROGRAM
              ALL USER IDs / ALL PROJECT IDs / ALL AREAS / NO PROGRAMS
                                 AMALGAMATED, INC.

            ------------------ FROM 01/01/85 TO 07/31/86 ------------------
            AREA NUMBER      USER ID        ACCESSES      HH:MM

            0                BILL           2             02:17
                                            -----         -----
                                            2             02:17

            5                BILL           1             01:02
            5                MARGE          2             05:08
            5                ARTHUR         2             10:01
                                            -----         -----
                                            5             16:11
                                            -----         -----
                                            7             18:28
```

```
WATCHDOG/PC DATA SECURITY                                                        PAGE 1
TUE 07/31/86  11:23 am                                           SORTED BY: PROJECT ID

                       AUDIT TRAIL DETAIL - COMPREHENSIVE
              ALL USER IDs / ALL PROJECT IDs / ALL AREAS / ALL PROGRAMS
                                 AMALGAMATED, INC.

                                          ----------- FROM 01/01/85 TO 07/31/86 -------
USER ID          AREA   PROJECT ID   PROGRAM  --------DATE---------   -----TIME-----  TOTAL
                                              IN            OUT       IN     OUT      HH:MM

Logon DEDE                USHER               03/23/86      03/23/86  11:43  11:50    00:08
DEDE              24      USHER      COMSVC   03/23/86      03/23/86  11:43  11:45    00:03
DEDE               2      USHER               03/23/86      03/23/86  11:45  11:50    00:05

*** SUB TOTAL ***         2 ACCESSES                                                  00:08

Logon MARGE               DELTA9              03/23/86      03/23/86  13:21  13:32    00:11
MARGE              2      DELTA9     COMSVC   03/23/86      03/23/86  13:21  13:30    00:09
MARGE             11      DELTA9     DGLA     03/23/86      03/23/86  13:30  13:32    00:02

*** SUB TOTAL ***         2 ACCESSES                                                  00:11

*** TOTALS ***            4 ACCESSES                                                  00:19
```

Report formats may be saved and reused. This feature is handy when you must prepare similar audit trail reports weekly or monthly.

Although security is the main purpose of the audit trail feature, the system usage information collected by *Watchdog* has other applications. For instance, usage data sorted by project ID can help you allocate costs to individual jobs or customers; and the record of program executions can help you decide which programs to keep on the hard disk, and which seldom-used programs would be more economically stored on floppy diskettes.

MAILBOX A flexible mail system lets you exchange confidential messages with other users. Group IDs may be created to simplify sending messages to more than one user. Menus and word-processor-like editing features make the Mailbox easy to use.

SYSTEM LIBRARY The system library feature provides for efficient use of your hard-disk space, while ensuring the security of your data. System libraries are directories set up to store programs and files that will be used from many areas on your system. *Watchdog* allows these programs and files to be resident in one library directory, and at the same time to be automatically accessed from anywhere on the system. Of course, *Watchdog* continues to monitor permissions and will allow only authorized users to access system libraries.

For example, your spreadsheet package may be placed in a system library where several users may access it. Meanwhile, you may keep personal files that you process using the spreadsheet software in your own private area. The benefit is twofold: the spreadsheet resides on the hard disk in only one directory for efficient storage, and your private files remain secure.

SYSLIB, a directory set up as a system library, is available to hold programs and files that must be accessible to all users at all times. *Watchdog*'s SYSLIB command directs library searches and allows not only program execution commands to be called, but also overlay and related data files.

STREAMLINED INSTALLATION AND ADMINISTRATION It is easy to put *Watchdog* up on your system. *Watchdog* may be loaded onto the hard disk or administered from the original distribution diskettes. You do not have to format your hard disk, or remove any data stored there before you begin. You may extend *Watchdog* security to existing directories by selecting them from a list of directories that are already on the hard disk. Protection is extended automatically to each chosen directory (and to any files and subdirectories it may contain) without having to move or copy files, and without having to create new directories. New directories may be created under *Watchdog*'s protection just as easily.

If you wish, take a "phased approach." Secure your most sensitive data first; your other files and programs will operate as before. Then, include this other information under *Watchdog*'s protection when it is necessary or convenient.

Setting system security characteristics, adding users, establishing new protected areas, and modifying file access permissions are all accomplished through *Watchdog*'s efficient System, Area, and User profile system.

WATCHDOG®

SYSTEM REQUIREMENTS

MICROCOMPUTER:

- IBM® PC AT™
- IBM PC 370
- IBM PC XT™
- IBM PC 3270
- IBM PC
- AT&T PC 6300™
- COMPAQ®
- ITT XTRA™
- ZENITH Z-150 PC™
- Any other 100% IBM PC-compatible machine.

DISK DRIVE:

- Diskette drive, 5-1/4″ double sided, double density (1 required)
- Hard disk drive (1 required). May be internal hard disk or add-on mass-storage unit.

MONITOR:

- Monochrome or color display.

PRINTER:

- Any PC-compatible printer with 80 or more columns.

OPERATING SYSTEM:

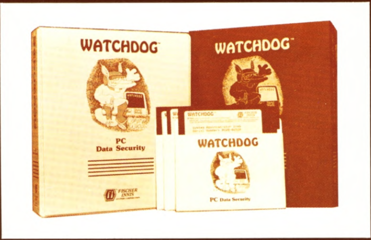
- PC DOS 2.0 or higher
- MS DOS™ 2.0 or higher (supported PC compatibles).

MINIMUM CONFIGURATION:

- 256 Kbytes RAM
- One diskette drive
- One hard disk drive
- One monitor.

WATCHDOG is a registered trademark of Fischer-Innis Systems Corporation.
IBM is a registered trademark of International Business Machines Corporation.
AT and XT are trademarks of International Business Machines Corporation.
AT&T PC 6300 is a trademark of AT&T Information Systems, Incorporated.
COMPAQ is a registered trademark of COMPAQ Computer Corporation.
ITT XTRA is a trademark of ITT Corporation.
ZENITH Z-150 PC is a trademark of ZENITH Data Systems.
MS-DOS is a trademark of Microsoft Corporation.

FI™ FISCHER INNIS
SYSTEMS CORPORATION



You've invested in a high-quality microcomputer to process your data. . . Now invest in a high-quality data security system to protect it. You can put *Watchdog* on the job today.

FI™ *FISCHER INNIS*
SYSTEMS CORPORATION

4175 MERCHANTILE AVENUE • NAPLES, FLORIDA 33942

800 237-4510 (TOLL FREE) ☎ *813 793-1500 (In Florida)*