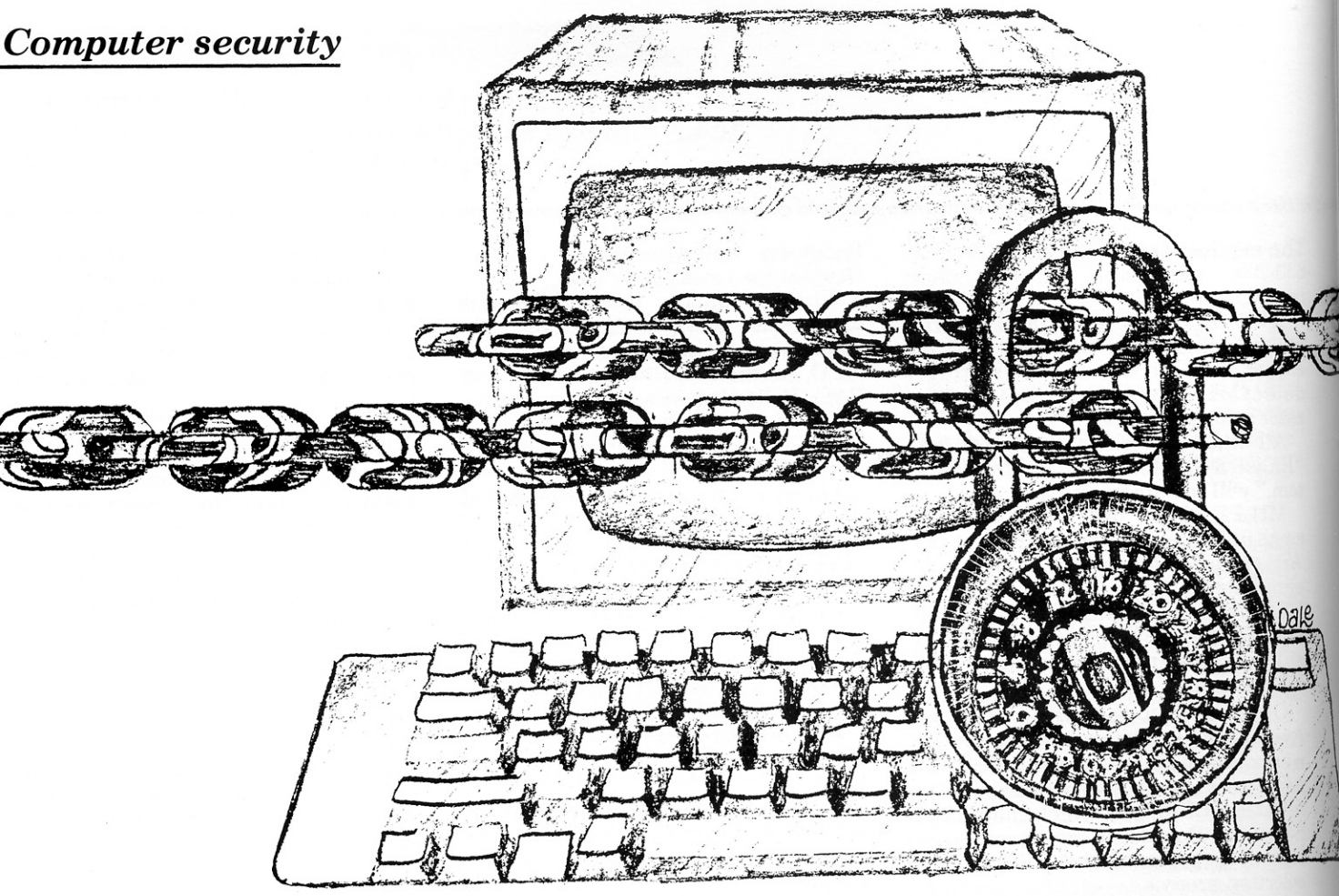


CW3 David E. Mann

The great mass of information being processed allows a misuse of computers and the information stored in them.
—USA ADP Systems Security Enhancement Program

Today's intelligence managers recognize the importance of both computer security and computing power, and they respect them both equally. We know that intelligence professionals have to move fast just to keep up with modern technology. Military Intelligence is on the cutting edge of microcomputer technology with the employment of personal computer (PC) systems in the workplace. Security of the information within those PCs is a hot topic which has not previously received the notice from upper management that it should.

Our ability to cope with computer security and vulnerable ADP areas is tied directly to the position taken by management with respect to use and misuse of PCs. The complexity of computer misuse is such that after years of debate, false starts and study, only recently has the US Congress undertaken a comprehensive proposal at the federal level to examine feasible computer crime deterrents.

The PC offers tremendous computing power, data storage and retrieval. It can be used as a stand-alone device or in a communications mode. The communications mode opens the door to a totally new way of doing business and presents a greater challenge for security.

Within the Army, concern over computer security has heightened with recent unauthorized accesses to government and commercial computers and the advent of the PC in the work environment. New equipment and communications networks have brought with them new vulnerabilities that must be considered. A large amount of sensitive information is available and potentially available to unauthorized users. We are looking towards the task of assessing the impact of the use of the new technologies and dealing with the COMSEC issues involved. We must define security in this new world of information services and develop strategies to meet these new requirements.

Personal computers:

illustration by Dale Hanawalt

a danger to classified information?

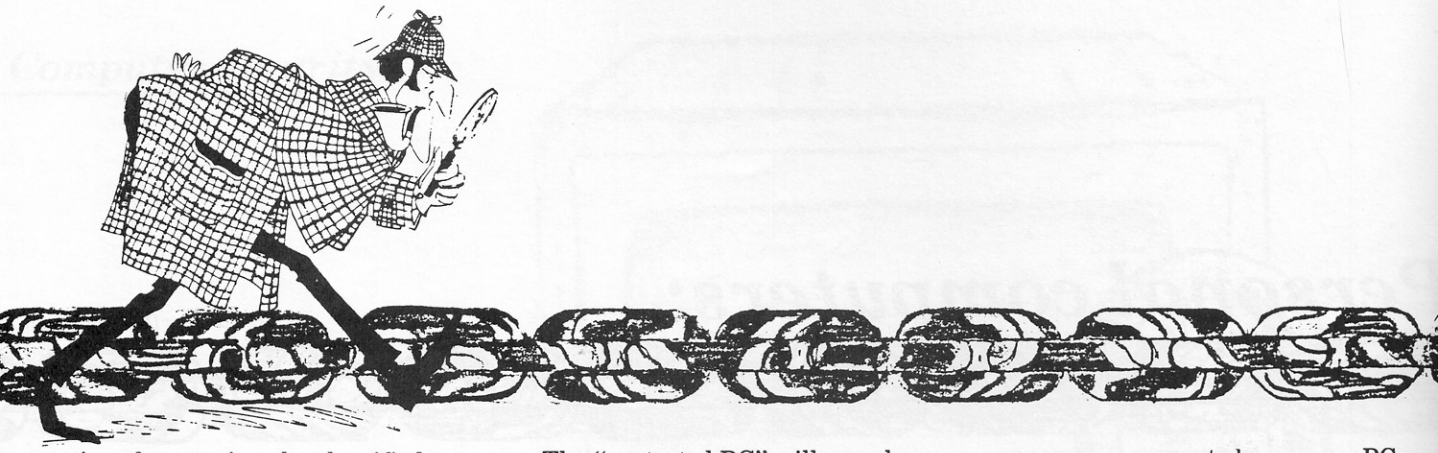
A recent study in computer security stated, "The great mass of information being processed allows a misuse of computers and the information stored in them. This trespass against information resources is ... a greater threat than the fraudulent use of computers ..."[1]

Security of PCs processing classified defense information is a different arena for the security officer than security of a large ADP facility. The basic elements of security practice remain, however, and by application of common sense measures together with support by management, PC equipment can return an even higher degree of security than that achieved by operating a mainframe system in a secure mode. This statement argues against a majority-held belief that PC equipment is more vulnerable than mainframe systems.

In contention is the idea that PC equipment applications are insignificant; that position states that since the PC is a stand-alone system, loss of data would not be significant. However, by realistically examining the contents of either a single PC or a network of several PCs, one finds that there is an inclusive data base of important information which is in many cases not duplicated, and thus it is vulnerable to loss or fraudulent manipulation. Physical access cannot be the sole concern of the security officer, but that concern tends to overshadow other considerations. A PC that is contained wholly within a secure area may contain, at any one time, either a large quantity of classified information, unclassified information or no information at all.

Security measures taken at a large ADP facility are different than those measures taken for the operation of a secure PC. However, the basic "practical application measures" of security work still apply to security for the PC. Currently, there are several approved PCs that have been tested for TEMPEST and which are listed on the National Security Agency's Preferred Products Listing (PPL).[2] PPL status makes those PCs and their printers which are listed useable in a common office environment. In practice, the TEMPEST approved PC can be plugged into a convenient electrical socket and operated. Assuming that all departmental and US government security regulations are met, the PC can come out of the packing box and be put to work processing classified materials immediately. The basic elements of security remain, however, and application of common sense security measures together with support from the commander must be present in order to insure a secure working environment.

Security managers can be lulled into a sense of false security by the



practice of extracting the classified diskettes or using a removable hard-disk (Winchester technology) system and locking those classified items in the security container. Although switching the machine off at the power switch is sufficient to neutralize all volatile memory locations, those machines equipped with bubble technology and other continuous storage systems must be treated as classified and thus secured.

Along with new equipment and communications networks, there are other vulnerabilities: large amounts of sensitive information can now become available to unauthorized users where previously that large data base was unexpected; security personnel simply did not think of a small "home computer" as the potential repository for megabytes of classified information. We are faced with the task of assessing the impact of the use of these new technologies and dealing with the security issues involved. We must define security in this new world of information services and develop strategies to meet these new requirements.

The October 1984 issue of **Business Communications Systems,** illustrated "A Protected Personal Computer" that incorporates such security features as a lockable, RF-shielded enclosure, a password and callback modem telephonic communications device. Use of an encryption circuit board using the National Bureau of Standards Data Encryption System (NBS-DES) provides on-line communications security.[3]

The "protected PC" will soon be found in many military offices. The commercial RF-shielded enclosure will be a TEMPEST approved PC instead; the entire workplace or building may be TEMPEST shielded in order to obviate the requirement for expensive TEMPEST treatment of hardware. The callback modem for telephonic communications will be identified as a protected wireline system[4] or otherwise secure telephone/data system. NBS-DES data security modules will be replaced by National Security Agency cryptographic systems designed for buss-level integration.

When the PC is operated in a secure environment (assuming that all standard security procedures are followed), personnel must avoid having a sense of false security. It is only good security practice to develop an operating environment which responds to external as well as internal threats. It is both good security practice and cost effective management of resources to correlate operating environment with the existing or proposed security environment. There are key questions which must be answered in order to formulate a security profile of the PC operating environment:

- Who really has access to the area?
- Who is the adversary?
- What are we trying to protect?
- What is the magnitude of the threat?

Traditional security measures will provide a large degree of protection for PC equipment and data media. There must also be a policy firmly guided by an experienced security officer that addresses such issues as the use of those PC systems for personal (private) processing with users exiting the secure area with media such as diskettes. The duplication of software (bootlegging), and the dumping of data and programs generated on secure PCs within the secure area to be taken home for use on privately owned computer systems, must *always* be prohibited.

While working in a secure environment, personnel must consider all potential security threats. The basic interrogatives (who, what, when, where and why) should be asked before setting up a new PC or network in order to obtain a profile of the operating environment.

Some problem areas mentioned in popular literature addressing PC security include management fears that the PC user may use his or her expertise to rise beyond that particular manager within the corporate structure. This fear stems from executives who may be insecure in their positions. Underlings have been known to use personal computer generated data to create conflicts within their organizations.

Unfortunately, many ADP managers consider the PC to be an emerging threat to their personal "ADP feifdoms". Obviously, they think, if someone with a PC can run a spread sheet of financial data or manipulate a listing of inventory items themselves, they wouldn't need the mainframe. These conditions create an atmosphere of internal office intrigue which can damage security.

Indeed, non-user friendly mainframe operating systems are sometimes deliberately maintained by the local ADP systems manager in order to discourage amateur users from having any interaction with the mainframe and thus making the ADP manager position indispensable. This is called "Establishment of the ADP

Guru" syndrome and ranks as one of the most vexing problems in the command's attempts to make computing within the organization efficient and user-oriented. Unfortunately, what this practice generates is the *ad hoc* processing of official data on privately owned personal computers. When that processing involves classified material, the problem is compounded by the lack of security for sensitive materials.

This problem is frequently seen by the security officer. Since non-ADP professional users attempt to process more and more information on office PC equipment, security violations increase. The increase in PC processing naturally also increases the amount of classified holdings, the size of the off-line, nonofficial data base, and the sense of urgency felt by action officers to quickly produce a classified product in what may be a non-secure environment at home on a privately owned system similar to the one inside the office for example.

Another area which worries management is the possibility that personnel will create their own data bases or historical files. This type of *ad hoc* data base usually proves impossible for management to control. A frequent fear among intelligence analysts and production managers is that someone will come out with an assessment based on his own private system's historical data, and the boss will assume that it is correct because it came from a computer.

Local area networks (LAN) and office automation (OA) are yet another area of data communications where a tremendous expansion is taking place. OA eliminates the staggering paperwork flow which action officers always experience. However, an OA which integrates telecommunications processing OCR electrical message transmission) creates a security and audit problem in control of data on the OA/PC network. The management opinion of such a system is negative; OA bypasses one of the basics of internal control: the chain of command.

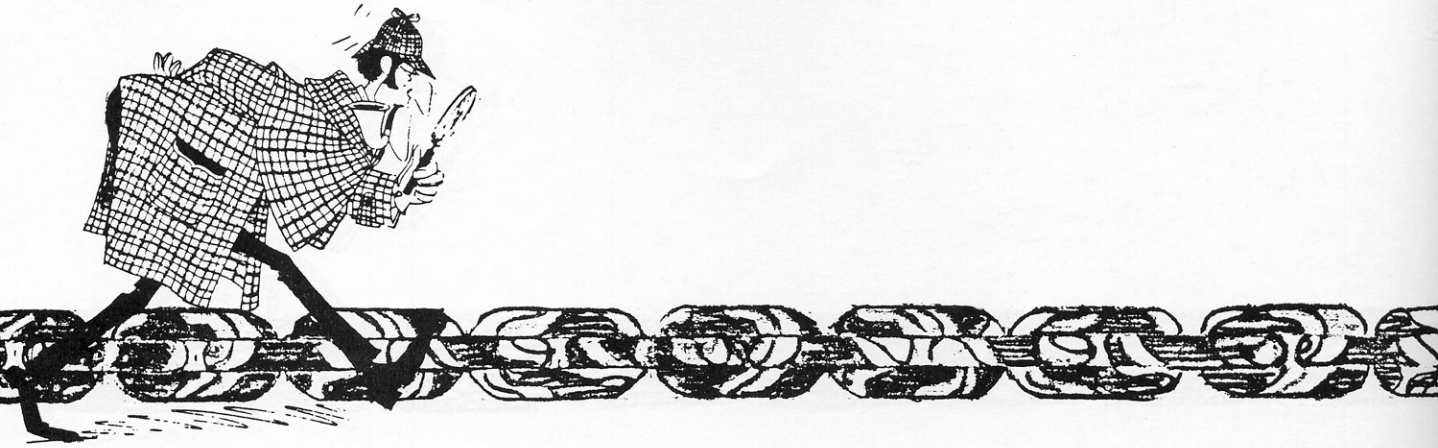
Offices usually have an administration area, with different personnel who initiate a transaction, process the transaction, then add the authority line or signature of the office chief. In other words, office managers have some built-in controls over what product leaves the office. With PCs linked together or using telephone modems, it is possible to compose messages, coordinate them as necessary, sign them, release them, and send them across the country to another office LAN without ever using a single sheet of paper. Such capabilities can only grow and expand in the future.

Loss of command and administrative control can be a product of LAN and multi-user/multi-level OA systems. However, software controls which limit the release authority of messages and the transmission of memoranda and other documents higher than a certain level in the management hierarchy are available to be used. Those controls put a stop note on certain documents and automatically route them to the boss for his or her review.

Theft of desirable supplies also reflects the growing population of home microcomputer users. For example, the 5.25″ and 8″ diskettes used by common word processing systems (Lanier, Wang, Xerox) can be obtained from Self Service Supply Centers and used on most home computer systems. Likewise, the printer ribbons for most "daisy wheel" printers can be used by the home hobbyist. Also, and certainly more expensive, is the exchange and theft of internal circuit boards contained within an office PC. Buss plug-in and serial interface circuit boards, memory expansion and bubble memory boards and other circuit cards are generally not accounted for by serial number. Indeed, many circuit boards do not have a serial number on them even though they cost, in many cases, hundreds of dollars. Once a personal interface board fails to operate, the user could simply bring it to the office PC, swap it with the office machine circuit card and take home a working board. The non-working machine is reported to the local repair facility, and the organization ends up paying for a circuit board.

Administrators wonder about the impact of personal computing on data integrity and control. Will the influx of microcomputers into the organization make it more difficult to keep data pure and well documented? The ultimate worry for the office administrator, of course, is software systems written for a number of particularly complex tasks and operated on an office PC without documentation.

This scenario for disaster reads like this: The writer of the programs was a whiz kid, a Mozart of the computer keys. However, the whiz kid also failed to document his or her programming. Documenting is considered by ADP professionals to be equal in importance to construction of a smooth running program. Documentation is accomplished on a PC system by writing down a comment about each and every program line of instruction. Those who had not participated in the writing of a complex program would find it difficult to determine the function of certain programming instructions or steps without consulting the person who actually wrote the instructions.



These are just a few of the security implications associated with the PC. If current TEMPEST requirements are applied to PCs, security problems should prove to be no greater than that of other communication equipment. Traditional security measures will provide a large degree of protection for PC equipment and data media. There must also be a firm policy on the use of those PC systems exiting the secure area with media such as diskettes, the duplication of software, and the dumping of data and programs generated on secure PCs within a secure area and their use in conjunction with a home computer system. Any programming done on the PC must be documented, with explanation of how particular modules and program instructions work, using a documentation module that is linked by logic to the main program.

Innovation is required in the application of security for networked systems operating within secure environments. For example, use of a TEMPEST approved PC with an approved telephone coupling device (MODEM) would permit transferal of data over a secure telephone or radio system. That exact same modem and radio or telephone could be used in a non-secure mode and transmit either classified or unclassified data to the outside, non-secure world.

The egress route that a signal follows from an OA system determines if the data transferal was permissible, even desirable. By taking an undesired route, that of classified information going out on a non-secure path, the data transferal would be totally unacceptable. The question for both commanders and security managers is: How do I make certain that the right path is used for the correct material?

The security officer should not delay progress; rather, he should find the ways and means to prevent the use of a non-secure system by accident or design. During the preparation of this article, I approached several security officers and asked them about their reaction to the example of the PC, MODEM and secure/unsecure communications paths. All of them viewed this situation with acute dismay and remarked that it was a security violation preparing to happen. They agreed that immediate action would be needed to nip the idea in the bud. Conversely, I questioned several action officers at DA level about their reaction, and they viewed such a system as manna from heaven and wanted to know when their offices would receive the system! Thus, it would appear that the type of security needed depends upon one's perspective and responsibilities.

Personnel planning modern systems must make certain they integrate the best possible mix of office systems and an efficient, user-transparent security operation.

ENDNOTES

1. *Report of USA ADP Systems Security Enhancement Program Lessons Learned FY 84, ADP Systems Security Division Security Support Detachment, 902d MI Group, Ft. George G. Meade, MD 20755, 1 Feb 84.*
2. *National Security Agency, "Preferred Products List," 4th Quarter, 1984.*
3. **Business Communications Systems,** *October 1984 issue.*
4. **Defense Intelligence Agency (DIA) Manual 50-3.**
5. *Department of Defense Trusted Computer System Evaluation Criteria, dated 15 Aug 83.*

CWO 3 Mann is the Technical Security Officer, US Army Special Security Group, Arlington Hall Station, Virginia. He has served in a variety of tactical and strategic assignments with MI since 1965. Before that, he was an Armor crewman. He has managed combined CI and COUNTER-SIGINT operations at tactical and strategic levels and has had numerous articles published in professional and civilian magazines. Mann has a BS in Criminal Justice Administration from The American University and is an MIWOAC and WOSC graduate.