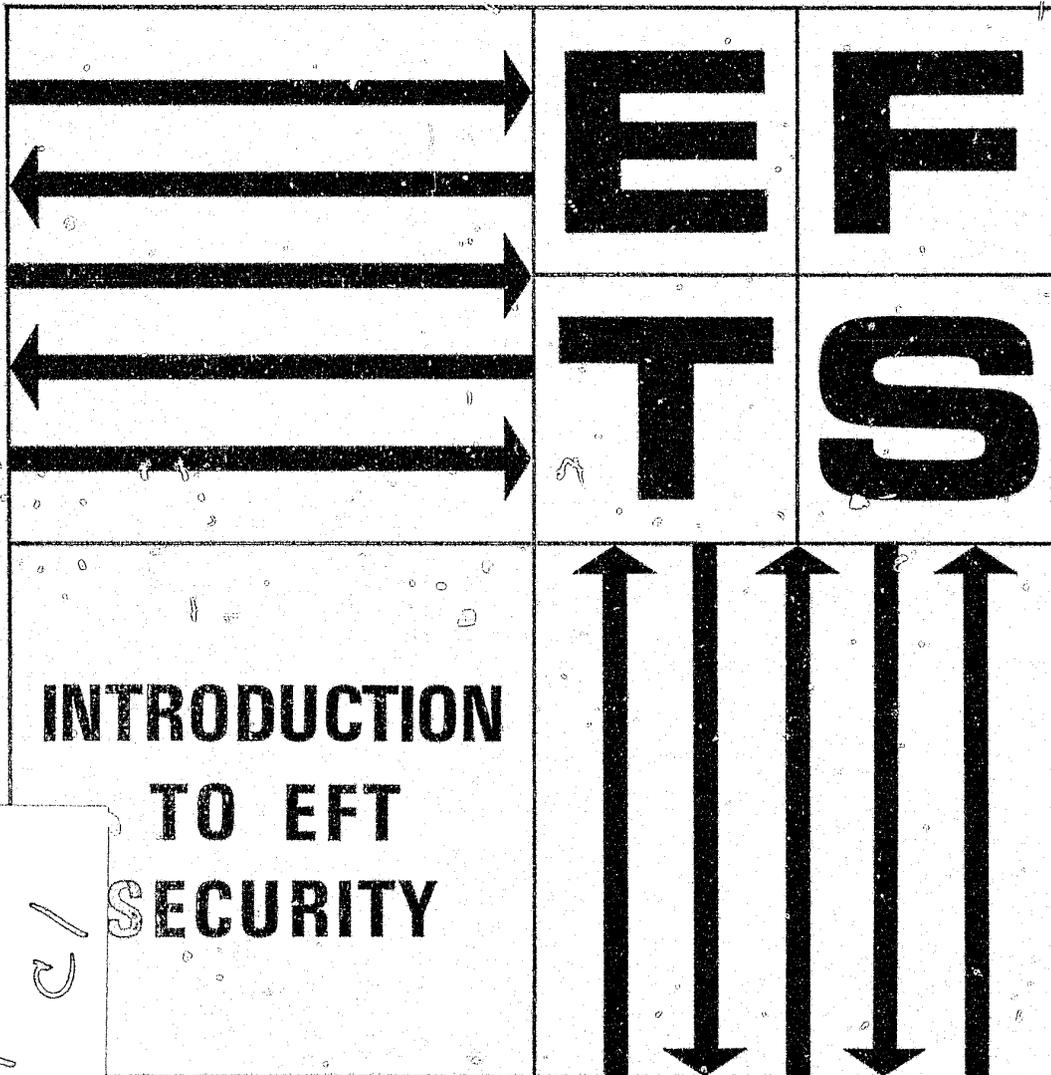




Prepared by Division of Management Systems and Economic Analysis, Federal Deposit Insurance Corporation, Washington, D.C. 20429



48899  
12/21

NCJRS

JUN 30 1978

ACQUISITIONS

INTRODUCTION TO EFT SECURITY

August, 1976

Prepared By

Division of Management Systems  
and Economic Analysis  
Federal Deposit Insurance Corporation  
Washington, D.C. 20429

## TABLE OF CONTENTS

1.0	INTRODUCTION .....	3
1.1	The EFT Security Risk .....	3
1.2	Risk Summary .....	3
2.0	IDENTIFICATION TECHNIQUES .....	5
2.1	Customer or User .....	5
2.2	Provider of EFT Services .....	7
2.3	Equipment .....	7
3.0	CARD SECURITY .....	7
3.1	Card Security Vulnerability .....	7
3.2	Countermeasures .....	8
3.3	Standards .....	9
4.0	DATA TRANSMISSION SECURITY .....	9
4.1	Introduction to Transmission Security .....	9
4.2	Transmission Security Vulnerability .....	10
4.3	Countermeasures .....	11
4.3.1	First Simple Cipher .....	11
4.3.2	Second Simple Cipher .....	12
4.3.3	The Time Value .....	13
4.4	The National Bureau of Standards Encryption Standard .....	13
4.4.1	Mechanics of Operation .....	14
4.4.2	Security of the NBS Algorithm .....	15
4.4.3	Criticism of the NBS Algorithm .....	16
4.4.4	Defense of the NBS Algorithm .....	16
4.5	Summary of Current Encryption Use .....	16
5.0	COMPUTER SECURITY .....	17
5.1	Introduction to Computer Security .....	17
5.2	Computer Security Vulnerability .....	18
5.2.1	The "People Threat" .....	18
5.2.2	Types of Crime .....	18
5.3	Countermeasures .....	19
5.4	Program Methodology .....	20

APPENDIX A—REFERENCES CITED

APPENDIX B—BIBLIOGRAPHY



F

4



.

.



## 1.0 INTRODUCTION

This paper is part of a set of papers devoted to the subject of Electronic Funds Transfer (EFT). The purpose of the paper is to provide the reader with some general background information on the subject of security in the EFT environment. In examining the technology, the paper attempts to identify the risks to security and those areas where this risk is high. It further touches upon countermeasures which can be implemented as protective mechanisms. In a future study on security, an analysis should be made of the likelihood that a breach of security could occur at any given point (or within any given subsystem) along the entire scope of the EFT network; an examination will then be made of the costs anticipated in securing all of the various components and subsystems that comprise the entire system.

In the EFT environment, security is broadly defined as the prevention of either the accidental or intentional disclosure, destruction, or modification of financial data. This broad definition would cover floods, fires, and natural disasters, as well as human error. For the purposes of this study, however, security is treated as the prevention of an unauthorized violation of or access to a financial system that results in the manipulation, modification, or destruction of that financial data, and more specifically, as a mechanism of protection against criminal abuse of the system.

### 1.1 The EFT Security Risk

The security risk in the EFT environment can be classified into two separate problem areas: first, identification, and second, penetration of the various subsystems.

In considering the first problem area, identification, there is a primary responsibility to identify the user of the EFT system. The current mechanism for identification is based on a two-key entry activator. These two keys are possession of a plastic card and knowledge of a Personal Identification Number (PIN). The identification requirement may also apply to the provider of the service and the equipment associated with the total system (see Section 2).

Penetration or violation of the subsystems is pictorially represented in Figure 1-1. The following are considered subsystems:

- the card
- terminals
- communications links
- the computer

Security considerations for each of these will be discussed in subsequent sections.

### 1.2 Risk Summary

Electronic Funds Transfer encompasses several primary components, consisting of Automated Clearing Houses (ACH), Automated Teller Machines (ATM) and Point of Sale Systems (POS). Since the risks associated with each of these components vary to some extent, the risk exposure as it applies to each separate component is shown in Table 1-1.

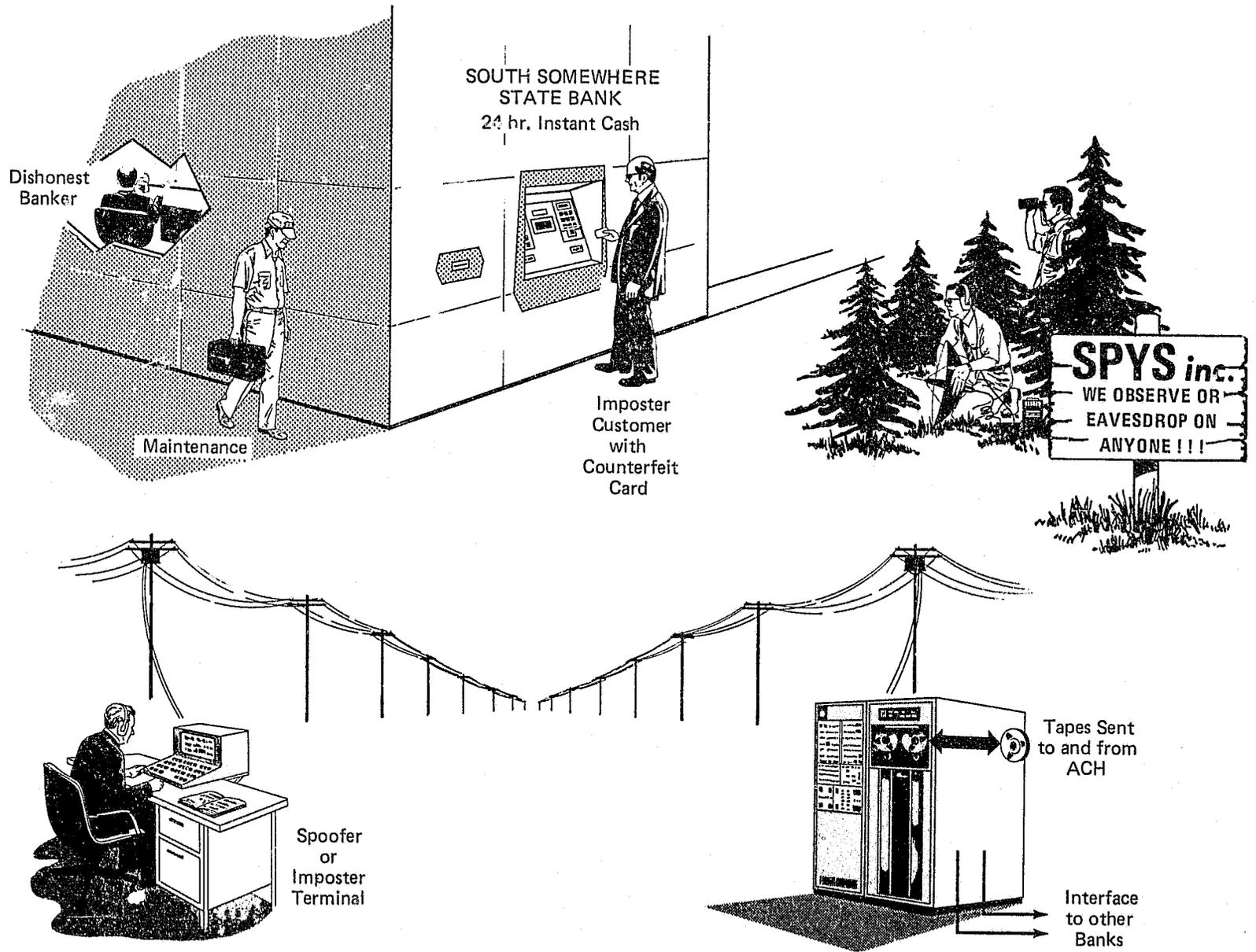


Figure 1-1 The EFT Security Risk



F

A



.

.



Table 1-1. THE RISK EXPOSURE

EFT Component	TYPE OF RISKS						
	Alter Transmission Tape	Data Link	Dishonest Personnel	Identification	Penetration of Computer	Physical Penetration	Radiation (information gathering)
A C H	X		X		X		
A T M		X	X	X	X	X	X
P O S		X	X	X	X		X

## 2.0 IDENTIFICATION TECHNIQUES

### 2.1 Customer or User

The identification of an individual using an EFT system can be accomplished in any of three ways:

- Who a Person Is
  - Personal Characteristics
    - fingerprints
    - hand pattern analysis
  - Behavior Characteristics
    - signature patterns
    - signature analysis
    - voice prints
- What a Person Has
  - magnetic striped plastic card
- What a Person Knows
  - PIN (password)

In the first method, who a person is, identification by machine can be accomplished by an analysis of various personal or behavioral characteristics. Techniques currently under development include recognition by fingerprint or hand pattern analysis, voice print analysis, and signature analysis. Unfortunately, these techniques are costly and have not been proven totally reliable. There are two types of errors currently associated with machine identification by these characteristics; these errors are granting access to unauthorized users and refusing access to authorized individuals. This problem is portrayed in Figure 2-1.

In the second method of identification by machine, what a person has, the identification is accomplished by checking for possession of a magnetic striped plastic card. Since it is possible for one individual to obtain another's card, this method by itself is not reliable and must be used in conjunction with either the first or third methods. The advantages of the second method are that it is relatively inexpensive and it is a convenient technique for inputting repetitive data into the system.

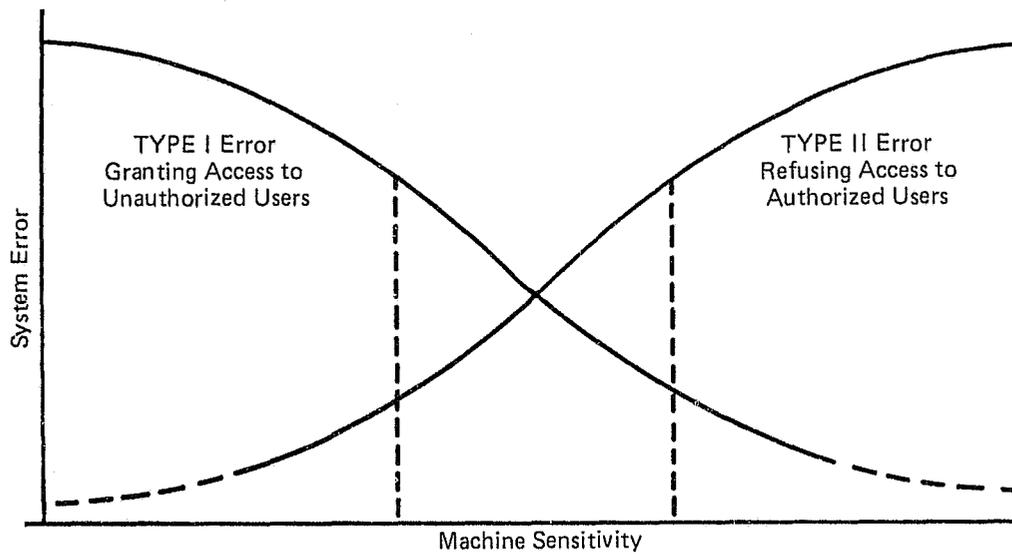


Figure 2-1 Personal Identification Thresholds

The last identification method, what a person knows, is predicated upon the password philosophy. In this case, the PIN becomes the key or password that the user needs to know in order to gain access to the machine.

Currently, entrance to the machine is determined by two of the above identification methods: possession and knowledge. The card and the PIN are referred to as the keys or activators to the EFT system. This system is vulnerable for several reasons. First, security of the PIN is lax. Customers have been known to write their PIN on the card. Consequently, if the card is lost or stolen, the individual who recovers it has possession of both keys to enter the system. Furthermore, customers may be indiscreet about entering the PIN into the equipment, allowing the PIN to be observed by others nearby. In one EFT/POS system, the customer tells his PIN to the clerk, who in turn inserts into the system. This verbal broadcasting of the PIN makes security of the number vulnerable.

Additionally, the PIN may be subject to electronic eavesdropping. If the wire is tapped, any kind of listening or recording device that is attached would be able to capture the PIN (if it were not encrypted). Table 2-1 shows the various techniques and associated problems related to user identification.

Table 2-1. USER IDENTIFICATION

	Current	Near-term Future	Long-term Future
Method	Magnetic striped card and PIN	Secure card and PIN	Fingerprint Hand Pattern Voice Print Signature
Problem	Vulnerable	Standardization	Cost Reliability

## 2.2 Provider of EFT Services

With the advent of modern banking and its philosophy of bringing banking services to the people, telephone banking is becoming a reality. This service allows customers to call their banker and have funds transferred from one account to another or to authorize bill payment. The funds involved in most of these transactions are small and identification of the provider of EFT services to the customer may not be warranted at this time. Except for the ability of one individual to recognize another by the sound of his or her voice, there is no mechanism in use today which would positively identify the provider of the EFT service to the customer.

## 2.3 Equipment

The EFT network consists of terminals which are linked to computers and computers which are linked to other computers. As shown in Figure 1-1, the installation of a spoofer or imposter terminal into the communications path has the potential to destroy the integrity of machine-to-machine communications.

A spoofer is a transparent electronic device whose existence is undetectable by either the terminal or the bank computer (unless special precautions are taken), and whose sole purpose is to defraud the bank by simulating the computer-to-terminal communication. For example, if a single instruction from the computer causes currency to be dispensed at an ATM terminal and the ATM does nothing more than interpret and carry out this command, tapping the communications link and issuing repeated dispense commands would result in substantial losses for each machine.

An imposter terminal is a device that, similar to the spoofer, is inserted into the computer-to-terminal communication line for purposes of defrauding the system. The imposter terminal is more complex than the spoofer, since it is not limited to communications with a single terminal, but can also communicate with the computer. An imposter terminal can therefore access the computer files and be used to fraudulently input to the central computer any financial transaction command present in the system. Potential safeguards for the spoofer or imposter terminal risk include installation of hardware and software to detect their presence on communications lines, and increasing the difficulty to duplicate communications between terminals and the central computer through encryption.

Specifically, if the information flowing between two pieces of equipment is coded such that only those two pieces of equipment are able to decode the message, then the integrity of the message can be guaranteed. Furthermore, the inability of a terminal (spoofer or imposter) to decode a message could be used to trigger an alarm notifying authorities that something is amiss in the system. The subject of encryption is covered in section four.

## 3.0 CARD SECURITY

### 3.1 Card Security Vulnerability

Counterfeit or duplicate cards represent an area of great concern, because no special knowledge of the data is generally required to duplicate a card. There are several methods of transferring magnetically encoded data from one card to

another. These methods vary by degrees of skill and expense, and the encoding quality of the duplicate cards ranges from being almost as good as the original to being not good enough to be accepted by most terminals.

The two most common methods of duplicating magnetically encoded data are skimming and buffer recording. One technique for skimming involves placing a piece of recording tape over the stripe of a good card and applying heat; the heat can be applied with a common household iron. Next, the recording tape is placed over the blank stripe of another card, and heat is applied again. Using this technique, it is possible to produce several duplicate cards without seriously degrading the information recording quality.

By contrast, buffer recording produces a duplicate card of higher quality, but this method is electronically complex and more expensive. Buffer recording requires an electromagnetic reader (a device similar to a tape recorder) and a buffer storage. The card is read and the data is stored in the buffer memory to later be written out on a blank card. Building an electromagnetic reader would likely require some knowledge of electronics and the good card's data format as well.

### 3.2 Countermeasures

In order to render cards less susceptible to duplication, some vendors are advocating the incorporation of secure card properties. This requires the introduction of some random property that will vary from card to card. One such technique utilizes two sets of magnetic bars, configured in an interleaved pattern and printed on the inner core of the plastic stock of the card. This would form a protective magnetic fingerprint and no two cards would be alike. The card could contain additional safeguards by incorporating heat sensitive and pressure sensitive materials that would invalidate the card if any attempt were made to alter or duplicate it.

Other methods being tested include the dilution of non-lethal radioactive isotopes into the plastic. Each card so produced would have a unique set of identification properties that could be machine read and computer verified, while still being extremely difficult and expensive to duplicate.

Figure 3-1 shows a typical card with its magnetic stripe format and secure card magnetic bar. The secure card properties should provide a guarantee against card duplication; however, this mechanism increases the cost of both the card and the card reader significantly, yet it protects only the card, not any other components of the system. The cost to read secure card properties increases in direct proportion with the number of random properties read. If only a few properties are added, the card is less expensive to read but relatively easy to duplicate. As more and more random properties are added, the card becomes both more expensive to read and more difficult to duplicate. An effective balance between terminal cost (reading cost) and the number of random properties to be read has not yet been determined. Perhaps for these reasons, coupled with the relatively small abuse of conventional credit cards, the secure property card has not yet gained widespread acceptance.

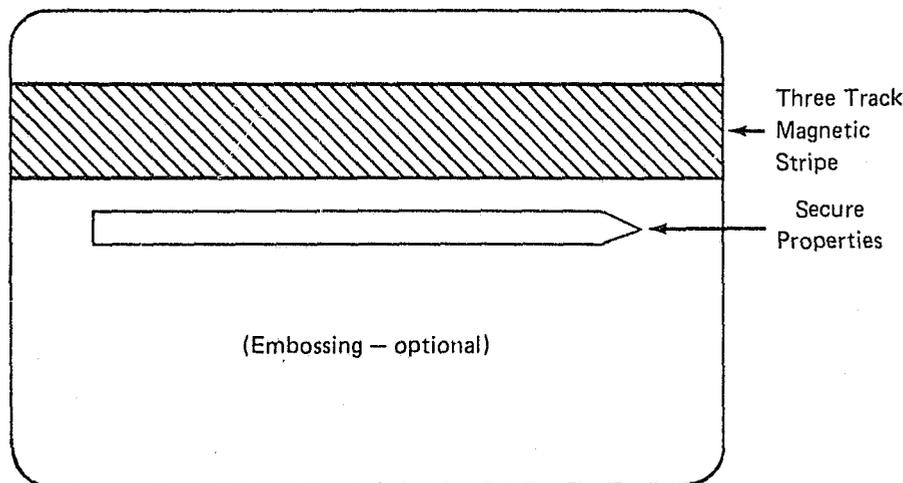


Figure 3-1. Typical Secure Property Card

### 3.3 Standards

There are several methods for protecting a card from duplication. Some of these techniques are the proprietary information of the organizations that manufacture and market them. Because of the cost considerations associated with various terminal reading capabilities, it would be highly desirable to have only one type of secure card property. This is especially true when considering EFT on a national network basis. The adoption of one particular secure card property as a requirement for all cards presents an obvious obstacle. It is believed that very little work has been performed to date in the area of adopting any one secure card property as a standard.

## 4.0 DATA TRANSMISSION SECURITY

### 4.1 Introduction to Transmission Security

In the on-line EFT environment, ATM and POS devices access and communicate with the financial data bases maintained by banking systems' computers. There may also be other computers or data concentrators in the network. These machine-to-machine links carry data and information consisting of PINs, customer account balances, deposits, withdrawals, and other financial transactions characteristic of the banking industry.

A simplified EFT system consists of three subsystems: the financial terminals, the data link, and the central computer. Data security has been concentrated primarily on only the computer and upon those who had access to it. The advent of machine technology has introduced other concepts into security considerations, especially the physical security of the ATM, dual control over posting, loading and other operational considerations, and all of the points addressed in sections two and three of this paper. With primary security considerations focused upon these areas, little attention has been given to the problem of data transmission security. Specifically, the problem of data transmission security addresses the issue of wiretapping.

Wiretapping provides a dual risk exposure to the system. First, it can provide a communication link to the individual terminal and thereby direct it to dispense cash to an unauthorized receiver (ATM), or it can authorize the sale of merchandise to an imposter customer (POS). The second risk is in the link back to the computer. Here the transmission link presents an avenue of approach right into the central file, and in this context, the traditional lock on the door to the computer room no longer exists. Once inside the computer, any of the weaknesses of the system are subject to criminal abuse, limited only by one's imagination and resourcefulness.

#### 4.2 Transmission Security Vulnerability

The communications lines are highly vulnerable. Almost without exception, the communication path between a remote device and the computer is via the telephone system. A cable directly connecting a terminal with the computer is always a localized operation and generally implies that the device and the computer are in the same building. Engineering characteristics of a direct connect cable are such that the distance between any terminal and its computer is technically limited. There are also financial limitations because the costs of long direct connect cables are prohibitively high. It is very unlikely that a given bank would develop its own communications system to connect remote terminals to its central computer. Therefore, since the technology exists for telephone connection of computer and terminal, and this technology is dependable, proven, and relatively inexpensive, the telephone system is the only reasonable and logical transmission medium.

Telephone lines are vulnerable in various ways. First, within every office building there is a focal point where all the telephone lines converge. In a room that is usually insecurely locked (if at all), there is a terminal board where all the phone cables are exposed. Since it is possible to gain access to this room, anyone with an understanding of the telephone company color-code wiring scheme could place a parallel tap on a line. This is significant since a telephone repairman would not be likely to detect the illegal wiring. It should be observed that this particular breach of security is common among New York bookies and other illegal gambling operations within the city. The following is the *modus operandi* of actual cases on record:

Bookies rent an office and have a phone installed. A parallel tap is placed on the line, so that the phone has an extension in some remote location. When the police are able to obtain the phone number and have it traced, they break into an empty room, while the bookies are still able to collect and place bets over the line from a location unknown to the police.

A second place in which telephone lines are accessible is through manholes under city streets or from the telephone poles and lines running parallel to the highways in rural areas. The significant point here is that the lines are physically insecure and can be breached at any one of a number of points. Instituting physical security for manholes or telephone poles is obviously impractical, and locking terminal boards would probably be ineffective. The vulnerability of telephone lines means that any signal on the lines can be intercepted or altered.

### 4.3 Countermeasures

Devices for accomplishing this are called spoofers or imposter terminals, both of which were described in section two.

If the lines themselves are not physically secure, then the data flowing on them must be coded. The subject of coding, or more correctly, cryptography, is the science of reading and writing secret messages. It is an old science, dating back to the ancient Greek civilization. The word has roots in the Greek words for both "secret" and "writing."

Cryptography is classified into three disciplines: invisible writing, codes, and ciphers. The study of invisible writing is not relevant to the problem of electronic data transmission. A code, in its generic sense, is a many-for-one substitution of linguistic characters which generally does not regard the length of the original word or group of words. In this case, a whole word or phrase is sometimes represented by a single letter. By contrast, a cipher is a one-for-one representation of the message, and it always conforms to the size of the original unciphered message. A cipher is the most applicable of the three disciplines to the problem of encoding electronic messages.

Ciphers may take any one of three different forms:

- Substitution. A substitution cipher involves the substitution of a single letter, number, or other character for the character being enciphered.
- Transposition. In a transposition cipher, the true letters of the message are taken out of their text order and scrambled in accordance with some predetermined pattern.
- Combination. The combination cipher involves a combination of substitution and transposition.

A useful product which pertains to codes and ciphers is the codebook. Codebook systems have been utilized by many organizations and nations for the protection of information. In the codebook, each word or letter is looked up in a table and replaced by the set of letters or numbers which appears opposite the word or character. Here, security of the message is dependent upon the security of the codebook.

#### 4.3.1 First Simple Cipher

To demonstrate how the simple cipher works, the following example is provided. The alphabet is printed in upper case, and its substitution cipher is printed underneath (note that the cipher has been displaced to the left by two characters; this displacement is known as the wraparound characteristic).

Alphabet: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Code: C D E F G H I J K L M N O P Q R S T U V W X Y Z A B

Coding the phrase:

Clear text: BLACK OR WHITE CAT

Ciphered text: DNC EM QT YJKVG ECV

The cipher is composed of an algorithm and a key. The algorithm is the mechanics necessary to code the phrase. In this example, the mechanics for the algorithm would consist of the instruction, "Shift the alphabet." The amount by which the alphabet is displaced, in this case by two letters, represents the key. This first simple cipher has one obvious disadvantage — with only a little bit of coded text, it is relatively easy to crack the code. Note that the letter B, for example, always translates to the letter D; the letter L always translates to the letter N; and so forth.

#### 4.3.2 Second Simple Cipher

It is possible to make the cipher slightly more complex, hence a little more difficult to crack. Consider the following example:

Alphabet:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Odd Code:	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
Even Code:	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

In this second simple cipher, there will be two keys: 2 and 4. In this case, the algorithm becomes somewhat complex, because it specifies that first the alphabet will be shifted by two for odd characters and then it will be shifted by four for even characters as shown above. An odd character means the first, third, fifth, seventh, etc. character in the message where a key of two is employed and the even character means the second, fourth, sixth, eighth, etc. character in the message where a key of four is used. To further complicate the code, no spaces between words will appear, but rather the characters XX will be inserted for what would normally be a space. The XX will also be treated on an odd/even character basis. The final requirement is that all lines of text or code will be 24 characters in order to give a block format. To fill any space which might result because a given phrase is less than 24 characters, characters from the end of the alphabet will be inserted as needed to make the line 24 characters in length.

As an example:

Clear text:	BLACK OR WHITE CAT
Block format:	BLACKXXORXXWHITEXXCATXYZ
Ciphered text:	DPCGMBZSTBZAJMVI <b>ZBEEVBAD</b>

Length: 24 characters

Note that in the word BLACK, the letter A is coded as a C, whereas in the word CAT the letter A is coded as an E. Note also, that in the word CAT the letter C is also coded as an E. Spaces between the words here are of two characters in length and are coded as BZ between BLACK, OR, and WHITE, but as

ZB between WHITE and CAT. In deciphering this phrase, the BZ/ZB and the BAD at the end will be disregarded by the cryptographer.

#### 4.3.3 The Time Value

The second example, somewhat more complex than the first, is still easily broken by a competent cryptographer. In fact, it is reasonable to assume that almost any code devised could be similarly broken, provided there was not a time deadline. However, most messages do have time value. For example, consider a message to a battlefield commander ordering a surprise attack on a city. Suppose, further, that this message is intercepted by the enemy and they immediately set to work to crack the code. If it takes them a sufficient amount of time to do this (assume that the code is broken two hours after the attack has commenced), then the cipher will be considered adequate. In general, the test of adequacy is not just the ability to break a code, but rather the ability to break a code within a specific time frame.

In considering the security of financial data, the time frame characteristic of the decoding process has relevance for fraud attacks aimed at a machine terminal or an individual's account. If the security consideration is to include an individual's right to privacy, then the time frame could be a long one. Therefore, the encryption would have to be safe for an indeterminate period. The time value for financial information and the costs incurred to protect data for specific time period have great relevance in the design of a security algorithm.

#### 4.4 The National Bureau of Standards Encryption Standard

The requirements of the NBS data encryption standard are unique. First, the encryption standard must provide for a high degree of security. Second, while the security requirement must not be compromised, the algorithm will be publicly known and readily available. This means that only the key will be kept secret. Third, the algorithm must be flexible in application. In this context, the algorithm was designed such that both government and industry will be able to use it for their own specific requirements. Fourth, the algorithm is part of the computer's hardware and completely independent of the software. The ramifications of this fourth point are extremely important, because hardware implementation alleviates the responsibility for software security requirements, thereby minimizing the likelihood that the algorithm could be compromised by programming. Last, the algorithm will be difficult to modify. This is necessary to protect the integrity of the network and to insure compatibility among all of the components comprising the system whole.

Some basic assumptions regarding the network environment are necessary. These assumptions are:

- Both authorized and unauthorized users have knowledge of the operation of the network.
- All internal mechanisms of a terminal (logic, memory, electrical connection, etc.) or any other associated hardware is physically protected from unauthorized access. All ATMs must meet the physical requirements specified by bank regulation.

- Physical access to the external controls of a terminal (keyboard, buttons, card input slot, etc.) is available to all users.
- There are individuals with the desire and technical knowledge to access a computer file to modify the data contained therein.
- There are individuals with the desire to gain unauthorized access to the network through authorized terminals.
- There are individuals with the desire to gain unauthorized access to the network through unauthorized terminals.
- Managers of the network desire to prevent the activities assumed in the fourth, fifth and sixth points above.

As was stated in section 4.3, encryption is the transformation of data from its original form to an encrypted or coded form. The NBS standard employs two basic transformations: permutation and substitution. Permutation changes the order of the symbols of the text or data. Substitution changes the symbols of the text by replacing those symbols with others. Combining permutation and substitution produces a complex transformation called a product cipher, which exhibits better cryptographic capabilities than either substitution or permutation used alone. A cipher that transforms a group of data bits into a group of cipher bits simultaneously is termed a block cipher, and if the algorithm operates on a fixed-length data block it is called a recirculating block product cipher.

#### 4.4.1 Mechanics of Operation

The new NBS algorithm is a recirculating block product cipher of block size 64 (64 binary bits) which utilizes a combination or encryption key of 56 binary bits. The algorithm is first based upon several permutations and a set of substitution tables specifying the transformation. Next, as shown in Figure 4-1, the permuted data is divided into two blocks (Designated L for left and R for right) of block size 32. The key is then entered into the system and combined with the text in the right half (the resultant being a function of the left plus the key operating on the right). This is designated in the drawing as R-prime. Data contained in the L-prime register is then transferred to the L register, while that in the R-prime register is transferred to the R register. This process is then repeated for a total of 16 cycles, after which the data is subjected to a function which is the inverse of the initial permutation.

Note that the encryption algorithm is a bi-directional device. Specifically, clear text inputted at the top flows through the algorithm and comes out as enciphered data at the bottom. Conversely, enciphered text inputted at the bottom flows upward through the algorithm and is outputted as deciphered or clear text.

The mechanics of the algorithm may appear quite complex to those not technically attuned to the world of electronics and mathematics. The most important point to derive from the above is that *time* is consumed in performing the mechanics of algorithm. This is important because it is this parameter by which the security of the algorithm can be measured. Using current technology, ciphering or deciphering 64 bits of text takes 40 microseconds.

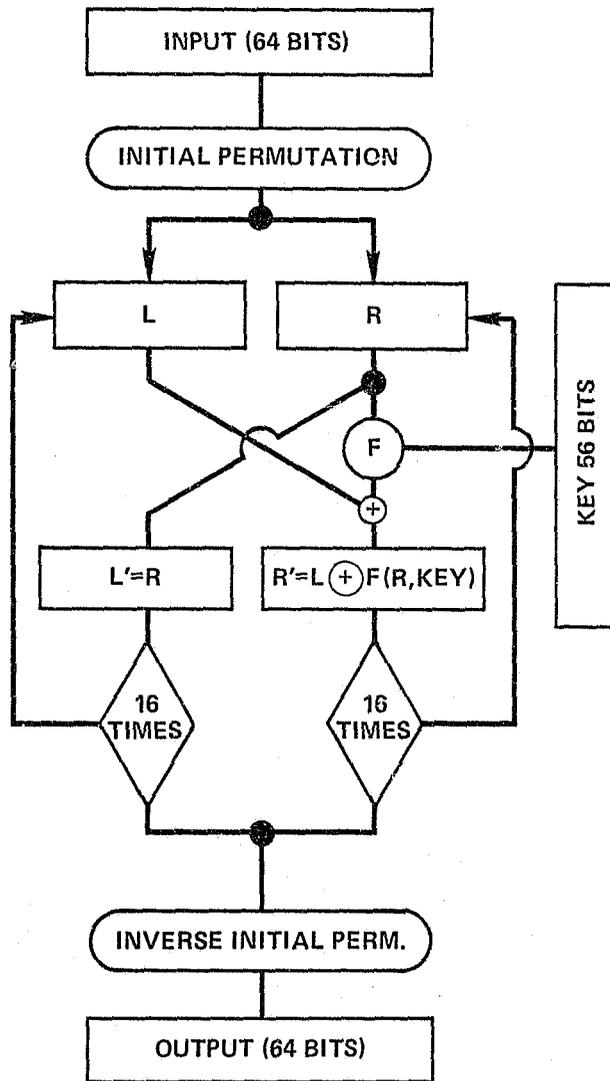


Figure 4-1 The NBS Encryption Algorithm

#### 4.4.2 Security of the NBS Algorithm

Since security of the algorithm depends upon security of the key, the algorithm security parameter is measured by the ease of obtaining the key. This can be accomplished through a technique known as exhaustive search. Exhaustive search implies a trial-and-error comparison for all possible combinations of the key.

In testing the algorithm, several assumptions will be made. First, a clear copy of text and a coded copy of that text are needed for comparison. Second, the algorithm is known, because it is in the public domain; but, the key used is secret. The methodology for this test is to initialize the key register (set it to 0) and then to try each combination of the key until the ciphered text agrees with the clear text.

The key length is 64 bits. Eight of these bits are used for parity (a check that is performed on data bits to test for transmission errors), so the combination is contained in 56 bits. Thus, there are  $2^{56}$  different and unique keys; it requires:

$$2^{56} \times 40 \times 10^{-6} \text{ seconds, or}$$

approximately two thousand years (under current technology) to test and compare all possible key combinations. A solution will be found on the average after trying half of the keys (half the time the key would be contained in the first half of all possible combinations), thereby reducing the time required for an exhaustive search for the key to one thousand years.

#### 4.4.3 Criticism of the NBS Algorithm

The example described above is predicated on today's technology, which requires performing each test-and-compare routine one at a time. Critics of the algorithm have suggested that technology in the next decade will have advanced such that it will be possible to process the algorithm in one microsecond rather than forty, and that as many as one million test-and-compare routines will be performed in parallel. If this is accomplished it will be possible to check all key combinations in one day through exhaustive search, or to break a code every half day on the average. This analysis leads to the conclusion that the algorithm itself is secure but the key size is too small and should be expanded to either 128 or 256 bits.

#### 4.4.4 Defense of the NBS Algorithm

The National Bureau of Standards contends that a charge of planned obsolescence is unwarranted and that the key size is adequate. They claim that even if one microsecond processing time could be obtained for the algorithm, a computer large enough to control one million processing chips in parallel does not currently exist and will cost at least \$100 million to develop. Furthermore, the cost for the processing chips is estimated at \$100 each. Combining the total cost of a million chips with the cost of the computer, a total cost for processing capability is roughly \$200 million. Depreciating this cost over five years yields a daily operating expense of \$100,000 which translates into an average cost of \$50,000 per key solution if one solution is found every half day on the average. This cost per key solution is only a minimum because it neglects to include the cost of the personnel and software necessary to support the operation. Additionally, there are technological problems to consider, such as the air conditioning needed to cool one million processing chips. The National Bureau of Standards believes that in time technological advance will improve the ciphering/deciphering capabilities somewhat, but not to the extent suggested by the critics. In conclusion, NBS feels that the current key size is justified and the security of the standard is more than sufficient for it to remain adequate throughout the next decade.

#### 4.5 Summary of Current Encryption Use

Table 4-1 is a compilation of ATM and POS vendors and their present mode of systems operation with regard to the use of security algorithms.

Table 4-1. VENDOR USE OF ALGORITHMS \*

	Uses NBS Algorithm	Uses Own Algorithm	Optional Capacity for NBS Algorithm	Does not use any Algorithm	Encryption Furnished as Standard Equipment	Encryption Optional Provided if Requested	Encryption Not Provided	
<b>Vendors of Automated Teller Machines (ATM)</b>								
B C N C		X			X			
Burroughs		X						
Diebold		X				X		
Docutel			X			X		
Incoterm		X	X			X		
I B M	X				X			
LeFeubre		X	X			X		
Mosler			X			X		
N C R		X	X			X		
<b>Vendors of Point of Sale Systems (POS)</b>								
Adressograph								
Multigraph		X	X			X		
A M F Electro System		X	X			X		
Anker Data System			Information not available at this time					
Data General Corp.			Information not available at this time					
Datatrol			Information not available at this time					
I B M			X			X		
N C R		X	X			X		
National Semiconductor			X				X	
Sperry Univac			Information not available at this time					
Sweda International		X	X					
Unitote Reytel							X	

\*See references cited in Appendix A

## 5.0 COMPUTER SECURITY

### 5.1 Introduction to Computer Security

Computer crime is defined as any act associated with computers where the victims have suffered or would have suffered a loss and the perpetrators of the crime either made or would have made a gain from their action. Today, computer crime is in the early stages of growth, and can be expected to increase significantly with the society's increasing reliance on automated services. As a result, the criminals, the types of crimes, the victims, and the types of losses are changing. This change is already evident in statistics collected from the areas of transportation, communication, credit cards and weapons development. It appears that the criminal continues to be attracted by the challenge and the large potential rewards, enhanced by a minimal chance of detection and an even lower likelihood of arrest, indictment, conviction, and sentencing. Many excellent works have been prepared on the subject of computer abuse

(see Bibliography). It is the intent of this section to provide some "food for thought" regarding vulnerabilities and countermeasures.

## 5.2 Computer Security Vulnerability

The vulnerability of a computer to unauthorized penetration is a function of the manner in which a computer is used. Originally, the computer was programmed for one application at a time (batch processing). Under these conditions, each program had access to all computer facilities as it was being run. Technological advances introduced the concept of multi-program processing system, thereby allowing several application programs to share a computer system simultaneously.

The introduction of multiprogrammed processing system led to the development of complex operating systems to manage both the job streams and the computer resources. Today time-sharing, real-time interactive terminal communications and computer-to-computer data links are all commonplace. All of these technological innovations, coupled with the growth of computer usage, have increased the risk exposure for computer abuse.

### 5.2.1 The "People Threat"

Any attack on a computer system is perpetrated by people. This "People Threat" is portrayed in Table 5-1. The table identifies those persons, or particular professions, that might be a legitimate threat to the system. Inclusion in this table does not imply that a particular group is necessarily dishonest; rather it is intended to show where the potential risk is located. This list is by no means complete, but indicates the nature of the problem.

Table 5-1. RISK PROFILE

	Programmer	User
Insider	Application Programmers Systems Support Programmers Operations and Maintenance Programmers	Tellers (Inquiry) Transaction Users
Outsider	External Subscribers Vendors	Customers Vendors

### 5.2.2 Types of Crimes

Some of the types of crime that can occur are as follows:

- Physical attack on computers  
One classification has deliberately been omitted from the Risk Profile table; specifically, the outsider who has no legitimate access to the system. This classification ranges from a sophisticated criminal with a highly technical background to the armed bandit who might physically attack a computer installation and hold it for ransom. This latter suggestion seems extreme, but such attacks have occurred on college campuses during periods of political unrest.

Given the hijacking and extortion schemes experienced by airlines, schoolbuses, etc., the possibility of an organized gang attack on a financial computer system should not be discounted. Physical security vulnerability is not limited to the physical penetration of the computer room, but also includes other acts of sabotage, such as setting the building on fire, flooding the building, severing the cables, etc.

- Attack on software and data  
Entrance into the computer system could occur through a remote terminal, a wiretap, or any of the computer peripherals, such as a card reader. This type of vandalism generally leaves the hardware unharmed, but could alter or destroy either the software or data that is stored in the system.  
Computer programs stored within the system are considered the property of the system or its owners. The theft of software or data, however, raises the problem of defining the theft since the program or data is generally not removed from the owner's possession but is merely copied.
- Theft of hardware  
This category includes the actual theft of tangible personal property and is traditionally classified as larceny.
- Theft of computer services  
This form of crime includes incidents where a person gains unauthorized access to a system and uses the system free of charge.
- Unauthorized surveillance  
Unauthorized surveillance introduces the concept of personal privacy and specifically deals with an individual's right to privacy and the use of a computer to violate that right.
- A combination of any or all of the above.

### 5.3 Countermeasures

After identifying the risk exposure in the preceding section, various countermeasures can be devised that could reduce or eliminate the chance of an attack. Some of these countermeasures, however, may not be cost justified. Before countermeasures are actually devised and implemented, it would be desirable to perform a risk analysis which correlates the following factors:

- Loss per risk attempt  
An analysis should be made of each vulnerable component to determine the actual losses that could be sustained if that component were violated. For example, the theft of an individual's card and PIN might result in a one-time loss of only \$100. Before designing countermeasures to protect against a particular risk, it is imperative to know exactly what the maximum loss would be were that component compromised.
- Cost to protect  
Another part of the analysis should determine the cost of countermeasures, including design, implementation and maintenance.

- Effectiveness of the countermeasure

The last part of this analysis should determine the effectiveness of the countermeasure. A countermeasure may not always be completely effective, as counter-countermeasures can also be devised. If, however, the mechanisms or methodology to defeat a countermeasure are extremely sophisticated and expensive, then the effectiveness of the countermeasure itself may still be quite high. For example, it may be known that the magnetic striped card can be easily and inexpensively duplicated. It is also known that various random properties can be introduced into the card that would render duplication more difficult. If only a few random properties are incorporated (to keep the terminal reading cost low), then the cost to duplicate these random properties may still be sufficiently high to discourage criminal attempts.

The design of the countermeasure involves balancing the risk exposure against the loss per risk attempt, coupled with the cost to design and implement the countermeasure. The correlation of these items would yield some measure of the effectiveness parameter. The need to perform this type of analysis is great, and further study in this area is recommended.

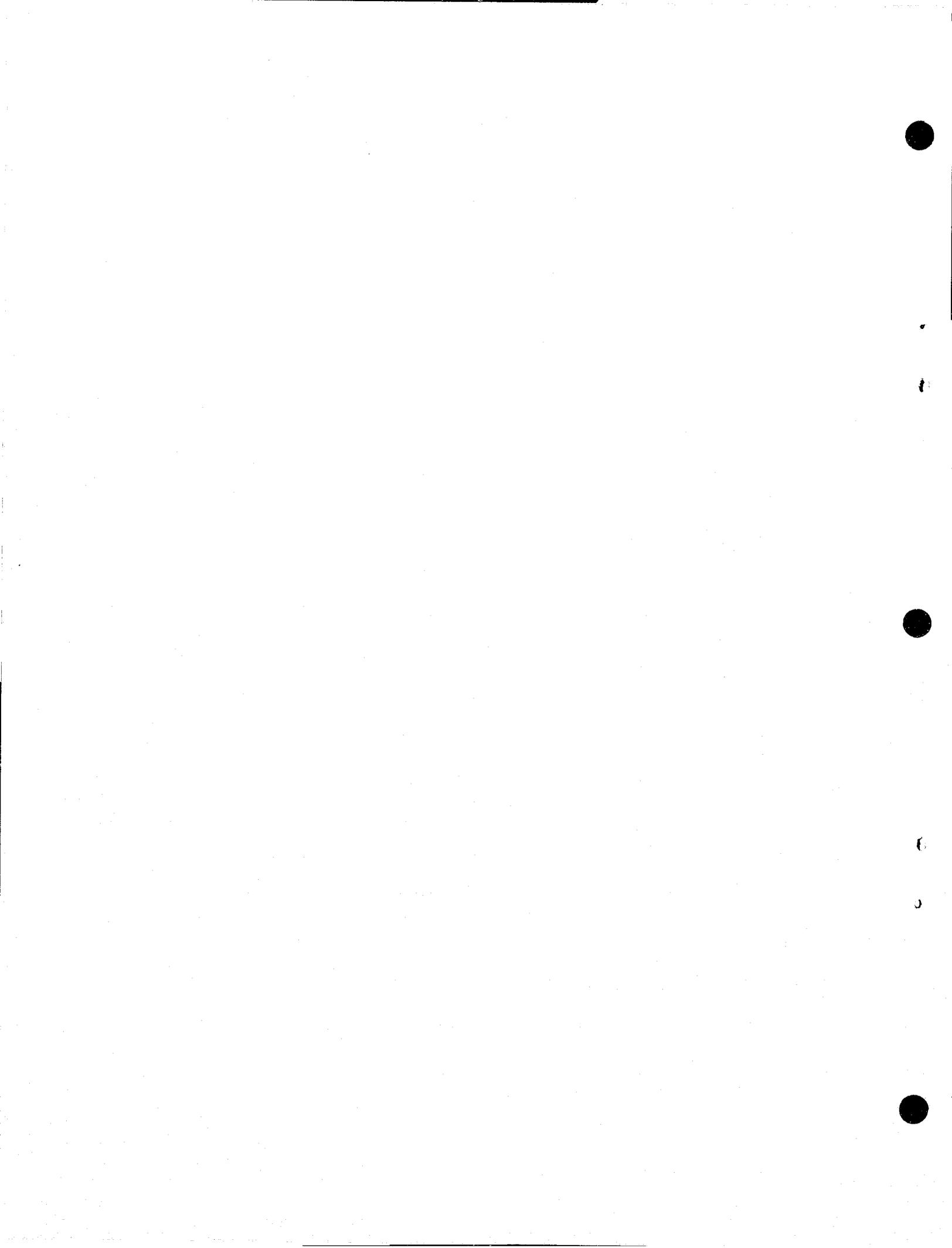
Attacks on software and data receive a great deal of attention within the scope of security protection. In this area, one important key to the protection of the computer system is fear of detection. Detection features can be made more difficult to subvert than prevention features and additionally, they can be placed anywhere within the system and moved easily from point to point. Parameters describing detection can be changed frequently, thereby making it extremely difficult for a potential criminal to discreetly enter the system and disrupt it.

#### 5.4 Program Methodology

The methodology of security protection should include a continuing research study so that evaluations and upgrading can occur continuously. It is recommended that such a study include the following activities:

- Enlarging the data base of reported cases of computer crime, including more in-depth investigation of the legal aspects of those cases.
- Producing validated models of computer crime to enable countermeasure experimentation in a cost effective manner.
- Assessing the danger and cost to society from computer crime relative to the degree of current and future control.
- Encouraging EDP organizations to support professionalism in computer and computer-related industries (for example, licensing or registration of EDP personnel with an ethical code similar to those used in medicine and law).
- Establishing penetration teams, whose function it would be to continually test systems in order to more accurately identify the vulnerabilities.

- Developing and using the computer itself as a tool to help control, prevent, or reduce direct abuses.
- Researching existing laws that are applicable to computer abuse and advocating legislation that will more precisely define computer crime.
- Calling for mandatory prosecution of computer crimes, a compulsory minimum penalty for those convicted, and detailed records to be kept of those prosecutions.



**APPENDIX A**  
**REFERENCES CITED**

1. Mr. Batters, T R W, Washington, D.C. Telephone conversation, June 18, 1976.
2. Mr. Paul Dunn, Mosler Safe Company, Milford, Ohio. Telephone conversation, June 18, 1976.
3. Mr. Leonard Fisch, Bank Computer Network Corporation, Chicago, Illinois. Telephone conversation, June 18, 1976.
4. Mr. Hall, National Cash Register, Dayton, Ohio. Telephone conversation, June 18, 1976.
5. Mr. James Lezenby, LeFeubre Corp., Cedar Rapids, Iowa. Telephone conversation, June 18, 1976.
6. Mr. Olson, Burroughs Corp., Detroit, Michigan. Telephone conversation, June 18, 1976.
7. Mr. William Pampers, Diebold Inc., Dayton, Ohio. Telephone conversation, June 18, 1976.
8. Mr. Douglas Williamson, Docutel Corp., Irving, Texas. Telephone conversation, June 18, 1976.



r

f



(

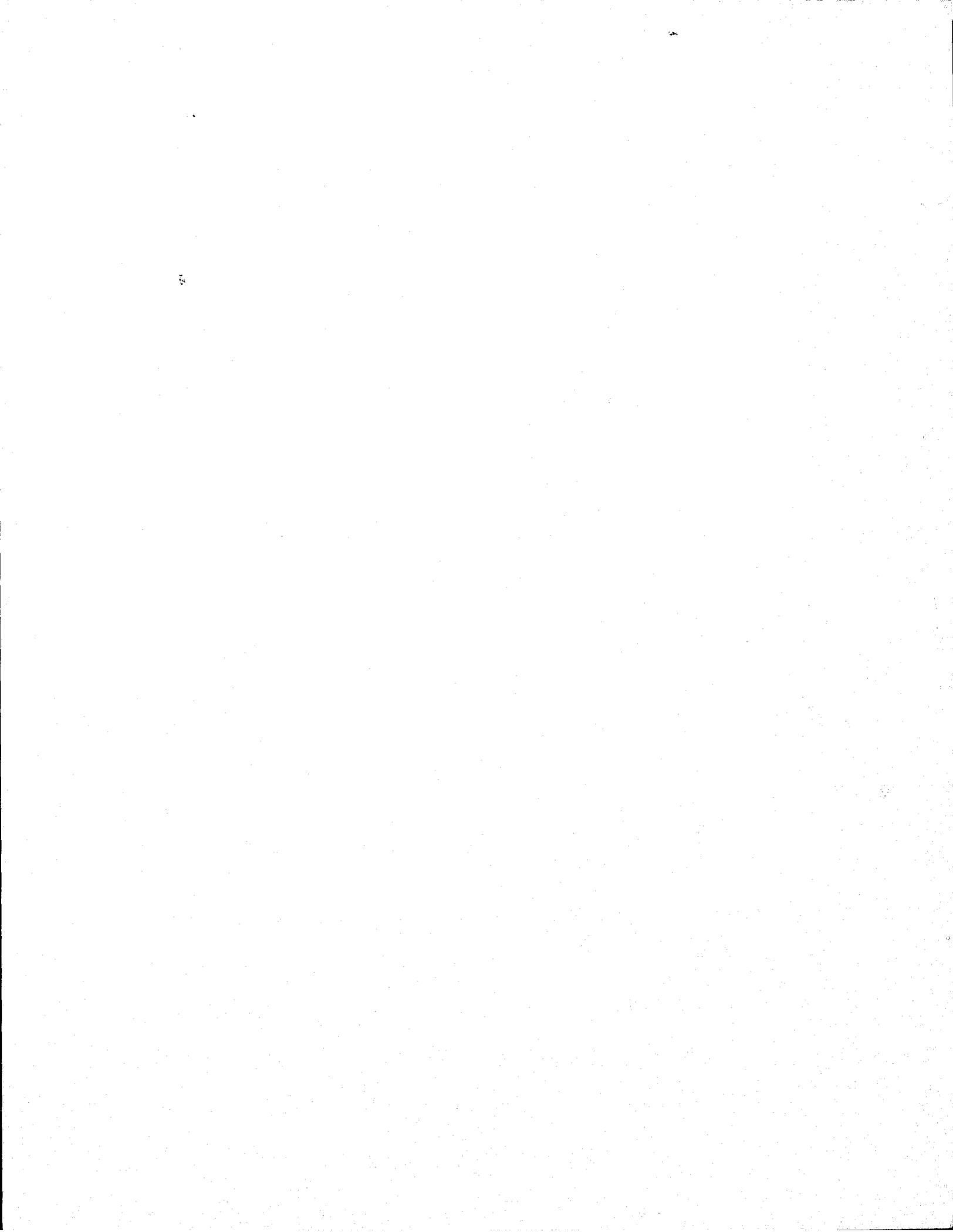
)



APPENDIX B  
BIBLIOGRAPHY

1. Allen, Brandt. "Embezzler's Guide to the Computer," *Harvard Business Review*, July-August, 1975.
2. Baker, Donald P. "Theft By Computer," *Washington Post*, June 16, 1976.
3. Bequai, August. "White Collar Crime and the Lack of Law as a Deterrent," special presentation, Federal Deposit Insurance Corporation, Washington, D.C., June 25, 1976.
4. Bransted, Dennis K. "Encryption Protection in Computer Data Communications," presented at the Fourth Data Communication Symposium. Quebec City, Canada, October 7-9, 1975.
5. *Computer Abuse*. Stanford Research Institute Publication #PD-231 320, November, 1973.
6. *Computer-Related Crimes in Federal Programs*. Report to the Congress by the Controller General of the United States, Pub. #FGMSD-76-27, April 27, 1976.
7. *Computer Security Developments Summary*. Information Systems Technology Applications Office, Electronic Systems Division, Air Force Systems Command, Hanscom AFB, Mass., Pub. #MCI-75-1, December, 1974.
8. *Considerations of Data Security in a Computer Environment*, IBM Pub. #G520-2169-0, July, 1970, White Plains, N.Y.
9. Diffie, Whitfield and Dr. Martin E. Hellman. *Cryptanalysis of the NBS Encryption Standard*, Stanford University Department of Electrical Engineering, 1976.
10. "Encryption Chip Set for Production." *Data Communications Magazine*, July-August, 1976, McGraw-Hill, Inc., New York.
11. *Executive Guide to Computer Security*. U.S. Dept. of Commerce, National Bureau of Standards, Washington, D.C.
12. Ferdman, M., D.W. Lambert, and D.W. Snow. *Security Aspects of Bank Card Systems*. Mitre Corporation, Bedford, Mass., September 1975.
13. Firnberg, David. "Your Computer in Jeopardy." *Computer Decisions*, July, 1976.
14. Flato, Linda. "EFT and Crime." *Banking, Journal of the American Bankers Association*, October, 1975.
15. Goldberg, Arthur G. and J. Milton Wood. "Special Presentation by the Finance Industry Marketing Group," IBM Corporation, Princeton, New Jersey, July 12, 1976.
16. Greenlee, M. Blake, and Robert V. Jacobson. *Computer and Software Security*, Advanced Management Research, New York, 1971.
17. Jeffery, Seymour. "NBS Data Encryption Standard," presented at the EFTS Strategies and Implementation Conference, April 23, 1976.
18. *Managers Need to Provide Better Protection for Federal Automated Data Processing Facilities*. Report to the Congress by the Controller General of the United States, #FGMSD-76-40, May 10, 1976.
19. Martin, James. *Security, Accuracy, and Privacy in Computer Systems*. Englewood Cliffs, N.J.: Prentice-Hall Inc., 1973.
20. *Mitre Report on Security Aspects of Electronic Bank Card Systems*, Mitre Corporation, Bedford, Mass.
21. Nycum, Susan. "Testimony of Susan Hubbell Nycum before the U.S. Senate Committee on Government Operations," June 23, 1976.
22. Parker, Donn B. "A Look at Computer Fraud and Embezzlement in Banking," *The Magazine of Bank Administration*, May, 1976. May, 1976.
23. Parker, Donn B. *Crime by Computer*. New York: Charles Scribner & Sons, 1976.
24. Parker, Donn B., Susan Nycum, and S. Stephen Oura. *Computer Abuse*. Special report prepared for the National Science Foundation, #NSF/RA/S-73-017. Stanford Research Institute, Menlo Park, California.

25. Piemme, Walter C. "Security Requirements for ATMs and Cash Dispensers," *The Magazine of Bank Administration*, October, 1975.
26. "Proposed Draft for Guidelines for Implementing and Using the NBS Data Encryption Standard," Department of Commerce, NBS, November 10, 1975.
27. Stiefel, Malcolm L. "NBS Standard Puts Encryption in DP Systems," *Computer World*, June 7, 1976.
28. Stiefel, Malcolm L. "Source-Data Automation," *Mini Microsystems*, June, 1976.
29. *The Considerations of Physical Security in a Computer Environment* IBM Corp. Pub. #G520-2700-0, White Plains, N.Y., October, 1972.
30. Woodridge, Susan, Colin Corder, and Claude Johnson. *Security Standards for Data Processing*. New York: John Wiley & Sons, 1973.



**END**