1990

# Network security: Risk assessment of information systems

Sher Lurain

Rochester Institute of Technology
School of Computer Science and Technology

# Network Security: Risk Assessment of Information Systems

by
Sher Lurain

A thesis submitted to
The Faculty of the School of Computer Science and Technology,
in fullfillment of the
requirements for the degree of
Master of Science in Computer Science.

Approved by: James E. Holiotis 9/5/90

Will J. Hall

Daryl G. Johnson 9/5/90

JULY 2, 1990

Title of thesis - Network Security:

Risk Assessment of Information Systems

I, Sher Lurain, hereby **deny** permission to the Wallace Memorial Library of R.I.T. to reproduce my thesis in whole or in part.

Date - September 5, 1990

TABLE OF CONTENTS

## ABSTRACT

This paper investigates fundamental security issues and the growing impact of security breaches on computer networks. Cost-effective security measures, such as asset-threat analysis, enable monitoring of security levels in complex systems. An evaluation of one technique, called the Livermore Risk Analysis Methodology (LRAM) is documented[1].

Untrusted communication lines, unauthorized access and unauthorized dissemination of information must be contained. The complexity and corresponding sophistication of todays' systems and the reliance of management on information generated by these systems make them attractive targets for computer related crimes. A profile of computer criminals and their crimes emphasize the importance of management involvement and social ethics as determents to crime. An overview of system security, control concepts, communication and transmission security, and a discussion of threats, vulnerabilities, and countermeasures is provided. The growing need for risk management models is presented as well as an overview of LRAM. Risk assessment of a specific system case study and risk profiles are developed using LRAM.

Keywords: Network security, authentication, access control, cryptology, data security, transmission security, passwords.

---

1 Guarro, Sergio B., "Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management", Computers and Security, North-Holland Publishers, 1987, pp. 493-504.

## INTRODUCTION

Information security can be thought of as the sum of computer and network security. In many respects, the interrelationships between the two are a function of the evolving digital technology. Network security development relies on existing computer security. One must acknowledge the vulnerability of systems that contain, control and process valuable assets. A secure system must restrict the flow of information to only authorized persons, protect system performance, and restrict the use of system resources to authorized persons and activities. Computer abuse is a negative consequence of the technology. "Our society must do something to control the problem. If not, our information system can't grow the way technology will allow us to.", says Ernest Conrads, the director of corporate security at Westinghouse Electric[2]. Donn Parker admits the unintentional and indirect consequences of the computer revolution will have the most profound and pervasive impact on society[3]. Social controls stemming from the computing occupations will be a significant factor in the development of professionalism from within the computing field. A code of ethics and a professional code of conduct is needed to establish and maintain public trust. Professional codes will also serve to deter computer abuse and the rise of potential computer

---

2 Hafner, Katherine, "Taking the Byte Out of Crime", REVIEW, October, 1988 p.60.

3 Hafner, Katherine, "Taking the Byte Out of Crime", REVIEW, October, 1988 p.66.

criminals. Studies show that only people with computer related skills and access will have the capability to engage in computer abuse in the future. The population of potential criminals may decrease due to the level of technology but losses per incident are destined to rise. Strengthening our existing laws can help deter the tide of potential criminals.

## II. CRIME METHODS AND CASES

"Computer crime is a typical example of a technological crime that utilizes the very nature of the technology to conceal the criminal act."[4] The new technology of today and the future includes robotics, voice data entry and output, expert systems, knowledge bases, portable computers and the automation of offices in the home. Presently the level of information security has not been sufficiently developed to handle these new technologies. However, even if we assume that the violators know as much as security specialists, there are many controls and safeguards that can be implemented to achieve a more acceptable level of security. Computer crime in the future will no doubt increase not only because of the increased reliance and proliferation of computers in our everyday lives, but due to the fact it is poorly reported and rarely prosecuted. Many cases never go to trial because of the embarrassment or unfavorable publicity it may generate. Crime will continue to flourish as opportunities increase to commit the crime and to be successful. Over half of present computer crimes are never reported.

The majority of computer crimes are perpetrated by personnel who have been granted access to the system. Access to valuable assets grants some individuals invisibility as no unusual actions would be necessary to commit the fraud. Their actions become a part of everyday routine. A typical example, is the creation of fictitious accounts which receive the

4 The First National Computer Security Conference, Computers and Security, North-Holland Publishers, 1985, p.65.

transfer of "round-off" fractions of cents from the interest calculation of a financial program. Here the altered program allows the perpetrator to withdraw large sums of money without being noticed.

What kind of people become computer criminals? Perpetrators tend to be white-collar amateurs between the ages of 18 and 30 years old, primarily males with unique skills, knowledge and access to the system[5]. Motives are as diverse as the ways computer crimes can be perpetrated. Some find it a personal challenge to find flaws in the defenses of a system. Negligence, power and authority, or malicious intent are also common motives. The most prevalent motive is financial gain by an individual or group of individuals. Greed and the desire to get ahead are strong motivations in todays' society.

In one study, few perpetrators were found to have previous criminal records[6]. They turned to crime to get back at an employer, to get even with somebody, to try to be someone, to get out of personal financial difficulties or to prove themselves superior to the computers. As far as detection of the acts is concerned:

> "It appears that perpetrators strongly fear unanticipated detection and exposure. This makes detection as a means of protection at least as important as deterrence and prevention. Perpetrators tend to be amateur white

5 Parker, Donn B., Computer Abuse, National Technical Information Service for Stanford Research Institute, November 1973, p. 49.

6 Farr, Robert, The Electronic Criminals, McGraw-Hill Book Company, New York, 1975, pp. 9-10.

> collar criminal types, for whom exposure of activities would cause great embarrassment and loss of prestige among their peers, in contrast to many professional criminals, who want their peers to know of their accomplishments."[7]

Computer crimes come in many shapes, styles and sizes. A recent survey based on 95 cases of computer fraud in the United Kingdom showed that in penetration schemes, 63% achieved their objectives by simply manipulating computer input and source documents[8]. Embezzlement from financial institutions can be accomplished by manipulation of records which are then used to conceal the actual theft. Embezzlement can include instances of changing credit limits, unauthorized program changes to delete items from reports, check processing of altered codes (MICR), creating non-existent clients or suppliers, illegal transfer of funds, granting excessive discounts or simply the creation of false records.

Another 12% of the cases used the computer to conceal a fraud trail. This could involve the disarming of detection devices as well as other system controls.

Unauthorized dissemination of information accounted for 7% of the cases. They used computer generated data to provide information such as dormant accounts, customer withdrawal habits and consumer lists.

---

7 Parker, Donn B., Computer Abuse, National Technical Information Service for Stanford Research Institute, November 1973, p.51.

8 Wong, Ken, "Computer Crime-Risk Management and Computer Security", Computer Security, Vol.4 No.4, North-Holland Publishers, Dec. 1985.

Unauthorized program changes perpetrated by fraudulent routines or by implanting a "Trojan Horse" were used in only 5% of the cases reviewed. A "Trojan Horse" is a software routine that does not contribute to the function of the program in which it is embedded, but rather exploits the legitimate authorizations of the invoking process to the detriment of existing security. A "trap door" is a special kind of Trojan horse that will execute only when certain conditions exist: for example, the Christmas chain letter that appeared on IBM mainframes in 1988[9]. Donald Burleson, a disgruntled employee, allegedly planted a program after he was fired that would wipe out all records of monthly sales commissions. The Texas securities trading firm discovered the break-in acouple days later, but after the loss of 168,000 records. He is awaiting trial for a felony involving the harmful access to a computer[10]. The victim company failed to apply some very simple security countermeasures. Controls on indentification and authorization procedures would have alerted personnel to Burleson's activities. The company did not change passwords and Burleson, as a security officer within the company, had knowledge of everyone's password.

Other simple countermeasures can prevent or mitigate potential losses due to fraudulent routines. Modification of code can conceal outstanding debt, suppress warning and

---

9 Cohen, Fred, "On the Implications of Computer Viruses and Methods of Defense", Computers and Security, North-Holland Publishers, Vol. 7 No. 2, pp.167-177.

10 Hafner, Katherine, "Taking the Byte Out of Crime", REVIEW, October, 1988, p.31.

control mechanisms, or permit other unauthorized actions. Authorization and documentation procedures deter this kind of fraud. Limiting the number of people who are authorized to change operating programs or internally stored program data can diminish the possibility of fraud. Classified information should be categorized by appropriate security levels. Request and approval of all program changes along with implementation, testing, feedback and confirmation will increase program integrity. However, control of program changes by authorized personnel is difficult to monitor. When computer programs contain the authorization and approval routines needed for decisions, such as returns or granting credit, it is also within the control of the authorized personnel.

Remote terminals were used in 15% of the cases to enter fraudulent transactions, to gain unauthorized access to information or abuse privileges given to authorized terminal users. The rise of remote terminal use increases the number of sources where incorrect input can be generated. To ensure computer files are not changed fraudulently from remote terminals, the number of terminals through which such changes can take place should be limited. Identification codes for each terminal and authorization codes for authorized personnel should also be used.

The remaining cases involved the stealing of computer time and resources. This would include the theft of computer hardware and software programs. It is interesting to note that most computer abuse cases are detected accidentally.

## III. NETWORK SECURITY GOALS

The functions of any security system are: avoidance, deterrence, prevention, detection, recovery and correction of unauthorized acts[11]. Due to the extreme openness of network system architecture and the high level of communications in current computer networks, detection is probably the most important weapon against infiltration. Detection techniques can be placed anywhere and parameters may be changed often to keep potential penetrators off-balance. The physical dispersion of data within the network environment and the issue of control mechanism placement makes implementation of controls no easy task. Access controls at every node can bring a high price and degradation of system performance. Protection of information from illicit dissemination and modification is needed to make the system secure. This task is complicated by the variety of equipment and the distances of interconnection in present systems.

No computer system can be 100% secure. Steps must be taken to analyze all possible security risks and the cost of protection against these risks. In networks, the highest area of risk is the data communications lines. Almost all communication transmissions are insecure and capable of being compromised[12]. Data interception is the most significant

---

11 Parker, Donn, Fighting Computer Crime, Scribner, 1983.

12 Rutledge, Linda and Hoffman, Lance, "A Survey of Issues in Computer Network Security", Computers and Security, North-Holland Publishers, Vol. 5, 1986, pp. 296-308.

risk to system security[13]. Telecommunication facilities give users opportunities for illegitimate access to databases. Prominent sources of data insecurity include spurious message injection, message reception by unauthorized receivers, stolen or deleted messages, disruption of service, noise vulnerability, disconnection of services and the rerouting of data to fake nodes. Message authentication will prevent instances of spoofing. In spoofing the intruder may alter the contents of messages in transit. When the attempt is made to decrypt the message, useless information is created. The user thinking that the encryption mechanisms is at fault may switch to clear text which is exactly what the intruder wants. Spoofing can be detected by feedback synchronization between the encryptor and decryptor. This can be done with the Data Encryption Standard (DES) that uses cipher block chaining and cipher feedback[14]. Any spoofing can be detected by the loss of synchronization.

According to Summers, Objective No. 1 in computer security is that information must maintain its integrity against inadvertent or malicious alterations[15]. A combination of encryption algorithms and protocols for message exchanges are useful countermeasures for these hazards. Note

---

13 Shahabuddin, Syed, "Computer Crimes and The Current Legislation", SIGSAC Review, ACM Press, Vol.5 No.3 (Summer 1987) pp.3.

14 Davies, Donald W., "Ciphers and the Application of the Data Encryption Standard", Tutorial: The Security of Data in Networks, IEEE Computer Society Press, NY., 1981, pp.3-16.

15 Summers, R.C., "Overview of computer Security", Tutorial by Abrams and Podul.

that network protocols can also be used as a weapon by an intruder to gain access or reroute network data. Security in networks differs from centralized computers. Switching nodes and concentrators are physically distributed and cannot be considered secure. The level of security attained in any system is limited to that of its weakest link. This is evident by a model of security proposed by Linda Rutledge and Lance Hoffman. Their model of security can be expressed as:

S = f(P1 * P2 * A * C1 * C2)
where: P1 = physical security
P2 = personnel security
A = administrative security
C1 = data communications security
C2 = computer security
S = total system security

Each element listed can be thought of as a variable with the value of zero to one. One represents the maximum security coverage and zero represents a total lack of security coverage. Because of the multiplicity of the model, if any one of the areas is deficient in security, then it is reflected in the total system security [16].

Encryption algorithms prevent unauthorized users from reading the data and replacing or modifying it without detection. The characteristics of a good encryption algorithm are application flexibility, a high level of security, understandability and availability. Keys must be protected from all threats of disclosure, destroyed when no longer needed, and securely stored. IBM developed DES out of their

16 Rutledge, Linda and Hoffman, Lance, "A Survey of Issues in Computer Network Security", Computers and Security, North-Holland Publishers, Vol. 5, 1986, pp. 296-308.

research on the Lucifer system. Now accepted as an Information Processing Standard, the algorithm has been approved for use by Federal agencies for use in unclassified computer applications[17]. Another, known as the RSA cryptosystem, is based on the difficulty inherent in factoring very large primes[18]. Considered by most to be very secure and practical, both can be easily implemented in hardware or software systems. Encryption can address many security risks. Some of these are computer resource access control, user and process authentication, detection of message replay, detection of unauthorized data modification or deletion, protection of proprietary software, prevention against disclosure of sensitive data and detection of errors. Key management is central to the success of any encryption system.

Objective No.2, is that sensitive and critical information must maintain its confidentiality against any intentional or unintentional disclosure[19]. Valuable data stored in computer files, for example: mailing lists, customer accounts, product plans, are a much sought after commodity in a growing and lucrative market. A policy, such as limited access to information based on the need to know, is one countermeasure that is easily implemented. Data should be

---

17 Davies, Donald W., "Ciphers and the Application of the Data Encryption Standard", Tutorial: The Security of Data in Networks, IEEE Computer Society Press, NY., 1981, pp.3-16.

18 Cohen, Fred, "A Secure Computer Network Design", Computers and Security, North-Holland Publishers, Vol.4 (1985) p.191.

19 Summers, R.C., "Overview of computer Security", Tutorial by Abrams and Podul.

classified by security sensitivity scales where highly sensitive or critical information should be stored in encrypted form and located in protected storage. Deciphering of the information would be needed to make it intelligible.

The problem of traffic analysis, allowing an interloper access to information by the detection of patterns of traffic in a network, can be solved by the introduction of noise over a communication line, either when no information is being sent or randomly injected to mask covert information flows. As long as there is no external difference between meaningful and random signals, no information can be extracted by an attacker[20].

Hardware security devices, policies and procedures, dedicated microprocessors and minicomputers can be used effectively as security watchdogs. Software packages such as Resource Access Control Facility (RACF) are effective tools in tightening security. RACF provides access control by identifying and verifying system users; authorizing access to system resources; and logging and reporting of unauthorized attempts to enter the system or access to protected resources[21].

The last objective of security, according to Summers, is for the continual availability of information and the

---

20 Rutledge, Linda and Hoffman, Lance, "A Survey of Issues in Computer Network Security", Computers and Security, North-Holland Publishers, Vol. 5, 1986, pp. 296-308.

21 Carroll, John M., Computer Security, Security World Publishing Co., Inc, Los Angeles, California, 1977.

prevention of unauthorized use or denial of service[22]. A popular game in time-sharing environments is to discover new ways to deadlock or crash the system. This denial of service causes the inability to process other users' work. Such an attack can cause severe damage. This means the impact of business interruptions could accrue losses developing from cash flow delays, production delays, stock shortages, missed or late deliveries, loss of new business or existing business or severe embarrassment to the organization. The resulting delays and inefficiencies within an organization can produce a loss of goodwill and public confidence that far exceeds any direct monetary loss produced by the original service disruption[23].

A significant threat to networks today is the computer virus. Usually, there is no outward sign of damage as it spreads unnoticed through a computer network. Yet, computer viruses are silent killers and can be highly contagious. Computer viruses are really just Trojan Horses with the capability to autorelocate and attack other programs[24]. The program enables a copy of itself to be implanted in a host. Under predetermined conditions the code is activated and some unauthorized activity takes place. This activity can be destructive causing records to disappear or requesting system

---

22 Summers, R.C., "Overview of computer Security", Tutorial by Abrams and Podul.

23 Parker, Donn, Managers Guide to Computer Security, Reston Publishing Co., Reston Va., 1981.

24 Davis, Frank and Gantenbein, Rex, "Recovering from a Computer Virus Attack", The Journal of Systems and Software, Vol.7 1987, pp.253-258.

resources for long periods of time. A recent virus infected computers across the country. A graduate student, Robert Morris, Jr., who intended no harm, allegedly jammed more than 6,000 computers. He has refused to discuss the virus issue on advice from his lawyers. The F.B.I. planned on launching a preliminary probe to examine whether or not federal law was violated, and reviewed the Computer Fraud and Abuse Act[25].

The worm apparently destroyed no data, but inflicted damage by reproducing itself and thereby slowing computers' processing speed and taking their memory. The Morris infection is estimated to have cost the University of Illinois more than $100,000 in lost computer time and time spent by experts to rid the system of the infection[26]. Morris had intended the worm as an experiment which would slowly copy itself across ARPANET and rest harmlessly in thousands of computers. Due to a programming error, the worm replicated more rapidly than planned. It was carried through the network disguised as a piece of electronic mail. Once inside the computer it would release a series of small subprograms. One instructed the computer to make multiple copies of the original program. One searched out the names of legitimate users and identified their secret passwords. Another told the computer to send copies of the original program to every other computer on its mailing list. Many security experts agree that this time we

---

25 Markeoff, John, "Innocent experiment went awry", The SUNDAY Tennessean, November 6, 1988.

26 Dresang, Joel and Werstein, Leslie, "Virus Shows Vulnerability of Networks", USA TODAY, Monday, November 7, 1988.

were lucky and people should view the outbreak as a warning. It should make more people aware of network vulnerabilities in the future[27].

Fred Cohen, a computing engineer at the University of Chicago, explained that the infection should not have come as a surprise. "For at least five years they have been alerted to the possibility of viruses. They were told it's inevitable. But they ignored the warning." He estimates that close to 100,000 computers have been infected with viruses in the past year. Cohen has demonstrated that given basic knowledge of a particular system, a virus can be constructed to infect enough programs so that an attacker could be granted system rights within a short period of time[28].

Morris's father, Robert Morris, Sr. who is employed as chief scientist at the National Computer Security Center, is responsible for shielding ARPANET from security breaches. As a witness for the House investigating computer viruses in 1983, Robert Morris, Sr. likened the creators of viruses and other computer pranks to stealing cars for the purpose of joyriding[29]. A House bill introduced in July 1988, would make it a federal crime to insert a malicious virus. Penalties for unlawful access to government computers or computers used by a financial institution include a year in

---

27 De-Witt, Elmer, "The Kid Put us out of Action", TIME, November 14, 1988.

28 Davis, Frank G. F. and Gantenbein, Rex E., "Recovering from a Computer Virus Attack", The Journal of Systems and Software, Vol. 7 1987, pp. 253-258.

29 Wines, Michael, "Dad's boast comes back to haunt him", ROCHESTER DEMOCRAT and CHRONICLE, Sunday, November 13, 1988.

prison and a maximum fine of $250,000. A prison term of up to 20 years can be awarded if fraud is proven. To date, the Federal government and 47 states have some kind of computer crime laws on the books. Only Arkansas, Vermont and West Virginia (July 1987) did not have any legislation specifically covering computer crimes[30]. However, legislation at the state level is neither uniform nor consistent[31]. Under the Computer Security Act of 1987, the National Bureau of Standards will determine guidelines for security standards. Standards would ensure an adequate level of security throughout the system. Legislation provides for the National Bureau of Standards (NBS) to develop a computer standards program which includes standards and guidelines related to security and privacy issues for Federal computer systems[32].

What can be done to fight against the growing threat of viruses? Many experiments and actual case studies have shown that from Bell-LaPadula-based protection schemes to the personal computer, no one is above a viral attack[33]. The Bell-Lapadula formal security model describes a set of access control rules by defining the notion of a secure state. It is the user with the least privilege that is the most dangerous where viruses are concerned. There is nothing to stop higher

30 Shahabuddin, Syed, "Computer Crimes and The Current Legislation", SIGSAC Review, ACM Press, Vol.5 No.3 (Summer 1987) pp.1-7.

31 Richards, Thomas, "Computer Crime Legislation Update", SIGSAC Review, ACM Press, Vol. 5 No. 4 (Fall 1987) pp.5- 8.

32 Ibid., pp.5- 8.

33 Abrams, Marshall D. and Jeng, Albert B., "Network Security", IEEE Network Magazine, Vol. 1, No.2 (April 1987), pp.24-33.

security levels from running infected programs written at lower levels or individual users from using infected software. A kind of isolation, using POset communication information domains and limited transitivity of information, help prevent the spread of unwanted viruses[34]. However, solutions that tend to limit widescale sharing, which is considered to be a valuable tool, are not attractive. Default protection mechanisms on files, cyptographic checksum procedures, backup copies, limited access, user notification and awareness cannot stop viruses but can aid in the detection and tracking of viruses.

34 Cohen, Fred, "On the Implications of Computer Viruses and Methods of Defense", Computers and Security, North-Holland Publishers, Vol.7 No.2 (1988), pp.170-171.

## IV. SYSTEM CONTROL CONCEPTS

In a distributed approach to security, total destruction would require multiple attacks. Although the opportunities for fraud are increased, this system of defense tends to minimize losses. The system allows geographically distributed divisions of an organization to operate under their own control. Each can communicate with a large central system and one or more of the other machines. The large central system keeps any information that the machines need to share. The distributed machines would continue to function and provide local service even if the central system was compromised. The control is distributed at the node level making the security of the system equal to that of the weakest node. With a duplication approach, systems can be duplicated to provide a "fall-back" system. Redundancy is a fundamental method of detecting errors and a means of providing back-up for components that may fail. This is a costly but effective approach, but the high risk of detection is a strong deterrent to fraud. Redundancy is used frequently in systems that demand high availability and cannot tolerate any system failure. In the last method, defense in depth, defenses increase in strength as the violator moves towards the center ring of defenses. These rings of defense work together to make the effort to access the information exceed the gain of the attacker. Most losses through fraud or error can be controlled by such interlocking controls. For example, access control mechanisms are usually layered. The outer ring is formed by the password

control system which stops unauthorized persons entry into the system. Sensitive files and data are protected by file attributes, usually done at file creation, which decides whether or not a person can read or write to certain files. Data base system access may require reauthentication of the user and encryption of sensitive data for adequate protection of information. At the application level, a decision to grant or deny access to programs or other resources can be made at run time as well as detect and prevent erroneous or fraudulent operations. Other software, including operating systems and telecommunications monitors, provide access and alarm controls which allow authorized users access to system resources. A well written program can be a very effective security tool. Management policies and procedures such as job rotations, security maintenance and the division of responsibilities will further assist reductions in exposures to risk[35].

Dedicated microprocessors are attractive as security aids for high volume processing and monitoring. For example, a database processor searches tracks for desired information. Only the output that does not violate the security specification is processed. The microprocessor can be used as a security controller by monitoring every access and I/O activity. This activity is logged and in the case of violation, a breach message or alarm is triggered.

Current hardware provides support for many security systems and the graceful degradation of the system when

35 Norman, Adrian R. D., Computer Insecurity, Chapman and Hall Publishers, New York, 1983.

something does go wrong. Hardware can provide support essential for logging and monitoring capabilities, execution domains, error detecting circuits and security kernels. The need to process multiple classification of data led to the security kernel concept[36]. It takes a small portion of the operating system and makes it accountable for enforcing security policies.

36 Ames, Jr., Stanley R., "Security Kernels: A Solution or a Problem?", Proceedings of the 1981 Symposium on Security and Privacy, April 27-29 1981, IEEE Computer Society, pp. 141-149.

## V. LOCAL AREA NETWORKS

Local Area Networks, or LANs, are composed of computers, modems, communication switches and links connected within a limited geographical area. From the users view, his personal computer integrates with the network, giving him computer and network capabilities. There can be many configurations for LANs. The primary advantage of all such systems is the ability to share resources. This ability also results in a substantial vulnerability. One must attempt to control the flow of information, both in the system and from the system. Systems' identification schemes attach unique identifiers to all components of the system. Files, programs and hardware are identified so that established access rules decide who can do what to which information[37]. The most common form of access control for the users is identification and password security. Authentication at login time is widely accepted. Computer networks maintain this identification and authentication control between hosts as users connect to other computer systems in the network. Protection of passwords, generation of passwords, user modification of passwords, internal storage of passwords are all considerations in a successful password system. Other systems such as voice prints, fingerprints, magnetic cards or badges, are popular in high security risk systems. Electronic card keys or "smart cards" are starting to be used as indentification cards for employees. They are programmed with personal data and

37 Carroll, John M., Computer Security, Security World Publishing Co., Inc, Los Angeles, California, 1977.

authorization codes. Still, these can be stolen. Voice prints and the like are biometric devices and considered by experts to be very secure. The strategy in any access control system is to prevent all unauthorized access while detecting and acting on all violations. The data integrity is protected by controlling the interactions and verifying that no data has been improperly modified or destroyed[38].

To lessen the chance of failure for access control systems, enforcing the "need-to-know" principle as criteria for access and dividing the responsibilities for authorization enhances chances of success. Employees should be allowed access to only those programs and files needed to perform their jobs. This deters casual browsing through a system. Too much authority in one person is dangerous. One person in charge of implementing controls can very well circumvent them. The rotation of jobs, surprise audits and inspections make collusion between peers less likely. Professional analysis and documented design procedures, such as structured walk-throughs, prevent many programming errors and possible fraud through modification. Master files should never be altered without some external checking procedure. Operating systems can be protected by providing read/write protection of data, restricting available documentation, not allowing diagnostic routines to circumvent security controls and restricting the use of an assembler[39].

---

38 Summers, R.C., "Overview of computer Security", Tutorial by Abrams and Podul.

39 Champine, George A., Distributed Computer Systems, North-Holland Publishing Company, New York, 1980, p.260.

In remote access, the logon procedure should be kept in read only memory or implemented in hardware to ensure the security of the system. It is also a good idea to lock out the user while the system is verifying his or her password.

Because LANs have the characteristics of microcomputer systems, on-line processing systems and distributed processing systems combined, control issues are paramount. LANs transmit information via "packets" or segments of data. Transmission control for LANs involve access protocols, which decide which station is granted the right to transmit over the data channel. Controls are necessary to guarantee transmission reliability. Each node must have the capability to authenticate messages arriving from other nodes. In a broadcasting scheme, consideration must be given to stations that might be monitoring transmissions broadcast over the common channel. One way to prevent problems, is to use end-to-end encryption.

## VI. AUTHENTICATION/ACCESS CONTROL

PASSWORDS. The dishonest or malicious person will find a way to compromise the protection provided with user identification/ password systems. It is only effective if its secrecy is maintained and the users change their passwords often. Employees may try to justify sharing their password with others to facilitate the sharing of data when in fact it destroys any value in tracking and restricting access. Password disclosure should be treated as a security violation. The recommendation for systems today is to change passwords on a monthly basis. In an automated system, changes every 10 to 15 days will not increase password overhead significantly, but will greatly improve security[40]. Persistent use of the same password by employees compromises the security of the entire system. Retire any invalid user identifications on a timely basis. This includes any terminated employees or when there is evidence of compromise. Distribution of user identifications and passwords can be encrypted and sent through a network or through conventional mail systems in double envelopes. Passwords can be used to control access to computer systems or to a particular data file. Usually access to a file demands a second password. Most password schemes today are poorly managed and offer limited security. Still, they are widely used and it is best to optimize their performance by several measures. Demand that the length of any password be sufficient

---

40 Mendus, Belden, "Understanding the Use of Passwords", Computers and Security, North-Holland Publishers, Vol.7 No.2, April 1988, pp. 132-136.

to abort exhaustive search attempts by an intruder. A password of 7 characters in length is reliably recalled by most people without the use of some memory aid[41]. User awareness of the safekeeping of passwords precludes writing them down somewhere. A longer password or machine generated password is more secure but harder for most to remember. By doubling the length of the password, the workload to guess it is raised by a power of 2. Shorter passwords are allowed in some systems but another problem arises. Most mechanisms will pad the shorter entries with blanks in maintaining the password table. An intruder will focus on these entries in the table and thus greatly reduce his efforts in compromising the system. The system should encrypt system password files and password comparison should be done while encrypted in a privileged mode to prevent compromise. There is some debate on the effectiveness of some encryption processes. Encryption processes in some of the earlier systems was accomplished by bit inversion that was compromised within a short period of time. To be effective, the encryption must raise the work factor to a high level making any attempt to derive the password from the table unrealistic[42]. The system should also limit guessing attempts, impose time delays between input attempts and disconnect after failed attempts. Turnaround delay is inherent in most individual attacks on password

41 Mendus, Belden, "Understanding the Use of Passwords", Computers and Security, North-Holland Publishers, Vol.7 No.2, April 1988, pp. 132-136.

42 Mendus, Belden, "Understanding the Use of Passwords", Computers and Security, North-Holland Publishers, Vol.7 No.2, April 1988, pp. 132-136.

tables. Some experts support disconnection after one failed attempt during a logon session. The system should reveal the least information to the user during a failed attempt. Monitoring and logon reports should be kept to facilitate history-keeping records for failed access attempts. This can be used to detect unanticipated attacks in the future. Frequent, random, but visible audits will deter potential perpetrators and safeguard integrity. Test protection mechanisms frequently and above all, impose sanctions against violators[43].

ENCRYPTION. Encryption is the reversible coding of data to conceal information. The theory behind encryption is to increase the work factor for the perpetrator beyond the value of the information it is protecting. Isolation barriers, erected by these encryption processes, establish protection of information by confusion and diffusion techniques. Confusion is accomplished by switching the characters of one message to another set of alphabet characters. Diffusion is accomplished by bit permutations of the message. There are many kinds of cryptographic systems, the simplest being substitution where the key becomes a permuted alphabet. Transposition, polyalphabetic ciphers, running key ciphers, shift register ciphers or combinations are the basis of other possible crytographic systems. DES uses primarily a block cipher with transposition and permutation of bits.

---

43 Norman, Adrian R. D., Computer Insecurity, Chapman and Hall Publishers, New York, 1983.

There are two basic approaches to communication security: 1) link-to-link oriented measures; 2) end-to-end security measures. Link oriented measures provide security through message protection on each communication link, with enciphering and deciphering applied to each link independently. Both protocol control information and the data may be encrypted. Link-to-link measures can thwart wiretapping but cannot prevent misrouting. The routing nodes of the network may attempt to steal or modify messages as they pass. A breakdown in security at any processor would compromise the system. To maintain adequate security at each node, key distribution costs and personnel to maintain a system of many nodes may prove to be financially prohibitive.

End-to-end measures provide uniform protection for each message from its source to its destination. End-to-end encryption prevents wiretapping of communications links and the introduction of false messages, as long as keys are properly assigned, distributed and controlled. Each logical network can use its own key, thus securing message traffic from alteration or compromise at intermediate routing nodes. Because the source and destination addresses are in plaintext for routing purposes, this method is more susceptible to traffic analysis. To insure message integrity, an error detection code, time stamp and sequence number can be cryptographically bound to each message block.

## VII. THREAT AND RISK ANALYSIS

OBJECTIVES. Threat and risk analysis is necessary to understand the nature of risks to the system and be able to relate them to the assets and potential asset loss. This enables system personnel and management to evaluate and devise effective controls and continue to evaluate them on a periodic basis. Any approach to risk assessment must attempt to account for all possible threat and loss combinations. The discovery and classification of possible exposures, whether critical or acceptable, benefits security awareness of users as well as policy decisions and the protection of assets.

MODEL. The Livermore Risk Analysis Methodology is a recent analytical and decision model for the application of security techniques. It was commissioned for development by the Air Force Logistics Command in early 1985. The approach does not attempt to derive a total risk measure, but instead focuses on the risk produced by individual risk elements (RE) in the occurrence of single event losses. The model can be described by the formula: (Refer to Figure 1 )

$$R\ [RE_i] = EF\ [T_i] \times PCF\ [PMCO_i] \times MPL\ [C_i]$$

That is, the annualized measure of the risk resulting from the i-th risk element (RE) can be calculated as the product of the expected frequency (EF) of the threat ($T_i$), times the probability of control failure (PCF) of the combined set of preventive and mitigative controls ($PMCO_i$), times the maximum potential loss estimated to result from the

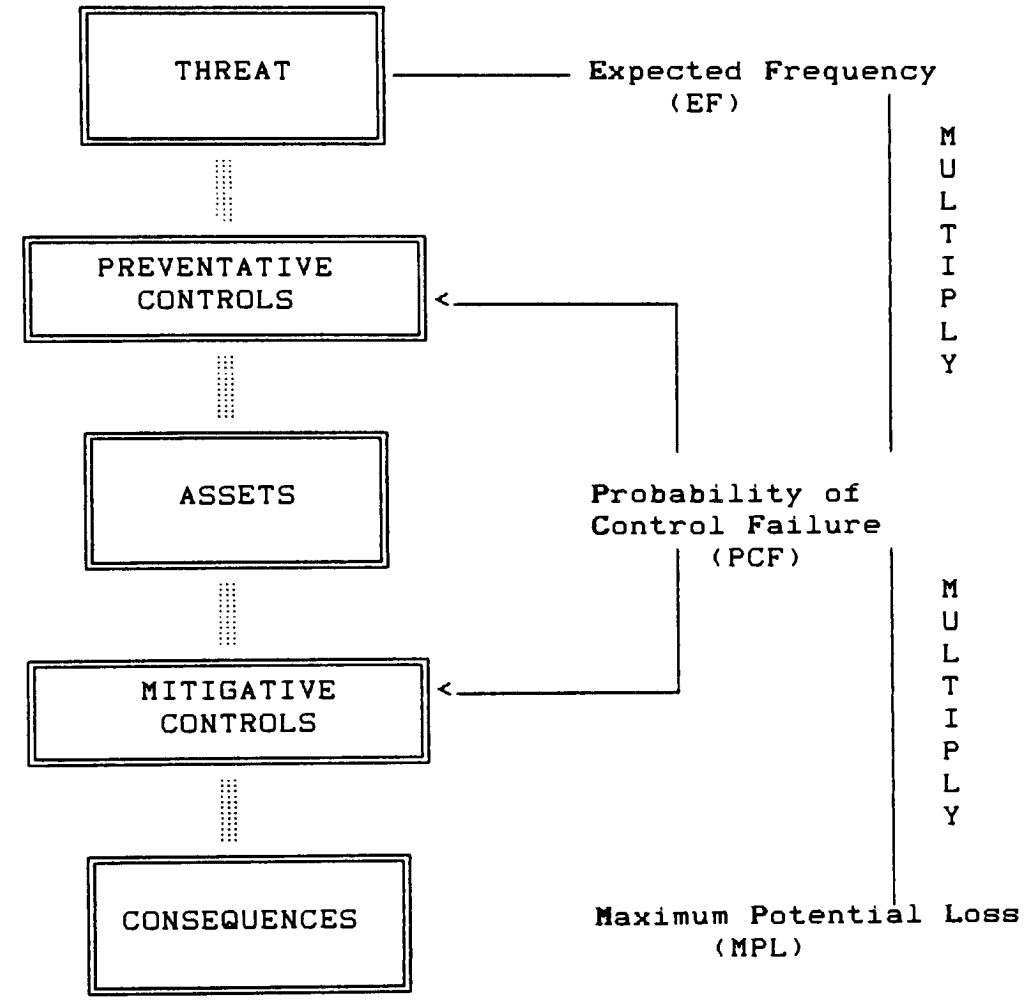



FIGURE 1. THE BASIC LRAM RISK MODEL*
RISK = EF X PCF X MPL

*Adapted from "Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management" by Sergio B. Guarro.

unmitigated consequences ($C_i$) of the threat on the assets[44]. The risk element (RE) becomes the product of three components namely, the threat event, the control failure event and the consequences. The three factor risk model reflects the actual threat to loss progression and separates the portion of the RE that can be influenced directly (controls) from that which cannot be influenced directly (threats). The upgrading of controls is easily accommodated by adjusting the probability of control failure value of the risk model.

PROPOSAL. A risk assessment will be performed by applying Livermore Risk Analysis Methodology to a specific system. This involves a detailed study of the vulnerabilities, threats, potential losses and the effectiveness of current security measures through the development of risk profiles. The risk assessment will render information needed to evaluate the methodology itself. Judgements of management, staff and co-workers based on their practical experience with the system and their instincts as to the perceived level of system security will be contrasted against the actual findings of the analysis. Any problems in applying the methodology or suggestion on enhancements will be noted.

The case study system is a VAX/VMS cluster processing environment used for decision support. The development of

44 Guarro, Sergio B., "Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management", Computers and Security, North-Holland Publishers, 1987, p. 495.

risk profiles will identify exposures and identify the present level of system security. Because of its proprietary nature, the results of any risk analysis are released to persons on the "need to know" basis. Every effort will be made to insure the organization's anonymity. In order to keep this material confidential, all the data collected and the results will be handled with the utmost discretion and stored in a stand-alone microcomputer. Management will be informed of all results. All assumptions and constraints to be imposed on the analysis will be identified in the preliminary stages. The wide area network will not be included within the scope of the analysis. The project will include all other components directly associated with the case study system. Constraints include the availability of data. The discussion that follows covers why this methodology was chosen, the procedures involved in the application of LRAM for risk assessment and the methods of data gathering to be used during the analysis. Afterwards, an overview of the case study system is presented.

LRAM. LRAM was chosen for many reasons. The methodology is a quantitative approach for the systematic identification and reduction of risk in information systems. Because it is objective, it is repeatable and can be used for risk profile comparisons. It is consistent with published DOD and NBS documents. The approach is documentable and very flexible, with the ability to be tailored to fit the size and complexity of any system and to the resolution and detail desired. The

wide scope of this methodology makes it capable of identifying losses as well as specific controls that would be cost effective. Practical and useful results can be obtained with a minimum of required resources. This makes a small-scale risk analysis possible resulting in a manageable set of risk scenarios. The procedure allows for efficient and meaningful reduction of material carried forward in the model-building process so only important issues and dominant contributors to risk are carried to later stages of the analysis[45].

My decision to use LRAM was reached after reviewing other risk analysis methods.

The IBM approach[46] uses order of magnitude estimations to calculate the total expected loss for any one system or file. Many calculations are needed for any one unacceptable event. The overall accuracy suffers from the high degree of guesswork and the manageability of the analysis in large systems is suspect.

The National Computing Center (NCC) approach[47] divides resources into critical and general categories. Critical assets are treated to a detailed analysis while general assets receive risk profiles containing more subjective judgements. Assessed losses are subdivided into direct loss to the installation, direct loss to users and intangible losses.

---

45 Guarro, Sergio B., "Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management", Computers and Security, North-Holland Publishers, 1987, pp. 493-504.

46 Wong, Kenneth K., Computer Security Risk Analysis and Control, Hayden Book Company, N.J., 1977.

47 Wong, Kenneth K., Computer Security Risk Analysis and Control, Hayden Book Company, N.J., 1977.

These losses are calculated at both the average and maximum levels. The LRAM approach endorses maximum level calculations to render conservative results. The NCC approach uses ranking of risks to separate individual risks in order of their significance. In the final stages of LRAM analysis only the significant risks remain. This helps conserve resources in an inherently time consuming process.

The statistical approach[48] requires copious amounts of data. The problem of obtaining accurate, available data and a resource intensive approach are the general weaknesses in this approach.

A checklist approach[49] is a pre-packaged list of potential vulnerabilities used for security audits. Security Audit and Field Evaluation (SAFE) is a low-cost approach to assessing risks and enabling management to take immediate steps to deal with security. Using this kind of methodology, it is questionable whether repeatable, useable results can be achieved. Although the provided checklist can be supplemented to reflect particular environments, it would be difficult for this method to support risk profile comparisons. The rating methods are variable and rely heavily on the investigator's subjective feelings.

48 Wong, Kenneth K., Computer Security Risk Analysis and Control, Hayden Book Company, N.J., 1977.

49 Krauss, Leonard I., Security Audit and Field Evaluation for Computer Facilities and Information Systems, AMACOM, 1972.

Donn Parker proposes several models[50] for assessing risk, allowing the user to combine approaches to fit their needs. In the Exposure Analysis Methodology, Parker defines the most important asset to be people. People are categorized by skills, knowledge, motivations and access to identified assets. The possibility of loss is based on the number of people who can produce a particular exposure. He contends that much guesswork is eliminated because the results are based on actual counts of people within an organization. This does assume that most risk is produced from within an organization and does not deal with threats arising from the outside. While an interesting approach, this could deteriorate in large organizations and become excessively labor intensive. Personnel donning many hats with overlapping skills could be hard to delineate.

Donn Parker also proposes a scenario technique. There is no elimination of non-important risks. The sets of vulnerabilities, scenarios and possible safeguards are ranked subjectively from the greatest risk to the least risk. Though results can be appended quantitatively through calculating expected annual loss, the methodology is primarily subjective.

LRAM is hierarchical in nature and is structured by three distinct phases[51]. Project Planning is the first phase and not much different than any other planning stage for any large

---

50 Parker, Donn B., Managers Guide to Computer Security, Reston Publishing Company, Reston Va., 1981.

51 Guarro, Sergio B., "Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management", Computers and Security, North-Holland Publishers, 1987 and conversations with the author.

project. Organization of team members and their responsibilities is not an issue for my application, but the scope and objectives of the project are.

The objectives include: identification and characterization of system assets/threats/current controls; identification of system specific risk scenarios and their contribution to overall security or a lack of security (existing vulnerabilities and their resulting severity); and evaluation of risk elements against an acceptability threshold to determine where additional controls are needed (adequacy of present controls). A clear understanding of the system environment and the proposed methodology is crucial to a successful project and meaningful results. An installation profile focusing on information assets, their location, usage, sensitivity, criticality and classification is the first important step. Information assets include information, hardware and related facilities that support information systems. Data was derived from several sources: system documentation, interviews with systems staff members, previous security reviews, historical and expert opinion and published data. The interviewees were questioned as to whom else I should interview and why. Work sheets were designed to meet the needs of the methodology and facilitate the progression of the project. These sheets also helped to document any decisions and give accountability for inputs. Each interviewee was identified by a random code so as not to divulge his/her

identity. All data collected was discretely handled and kept confidential. Sample worksheets are located in Appendix I.

The next phase, Risk Analysis (RA), was composed of three separate stages: (1) Information gathering and management input-IG, (2) Risk element definition and screening-REDS, and (3) Risk acceptability assessment-RAA. The methodology suggested that information gathering is best done during those stages in which the information was needed. Information was gathered throughout the model; the input items of concern were addressed when that section of LRAM was discussed.

The risk element is the basic unit for risk analysis. Assets and their applicable consequences were used as a starting point for the definition of risk elements. A risk scenario, the possible relationship between a threat and an asset, describes a threat-asset pair. A threat is the source or "initiator" of a potential danger. The propagation path and loss consequence can be thought of as qualifiers which delimit the pair. These four elements combine to form the unit known as a risk element (RE).

The IG stage created several lists from the identification and evaluation of assets. The asset list was organized hierarchically. The appropriate level of detail determined collectively by the level at which control decisions were made, the amount of resources available, and the levels used in previous analyses. Assets were characterized by classified, critical, sensitive and cost or value attributes. At this point, the attributes were needed

for categorization of assets and development of a system-specific asset list. This became the driver of the model and provided the structure needed to organize work sheets, easily locate information, and defined the level of detail necessary. Assets with monetary value only were identified. The level of materiality determined the number of monetary assets that were examined in the risk analysis. This monetary level was based on discussions with management. For the analysis to remain cost effective, the list must be manageable. If a major asset is material (important) and needs to be included in the analysis, this could help set the materiality level. The sensitivity and criticality of data and/or system resources are categorized and not subject to materiality screening. They are carried forward to the RA phase. Generic loss consequence identification, indirect or direct loss, was compiled. Generic consequences were screened and ones not deemed important or credible were eliminated. Some examples of generic consequences are disclosure of data, destruction of data or the denial of service.

The REDS stage resulted in the creation of specific initiator-asset-path-consequence sets. (Refer to Figures 2A and 2B.) In the first pass, generic risk elements (GREs) were defined and in a second pass, specific risk elements (SREs) evolved.

After major consequences were identified, material assets and major consequences were paired and defined as asset-consequence elements. As an example, let a DBMS be the

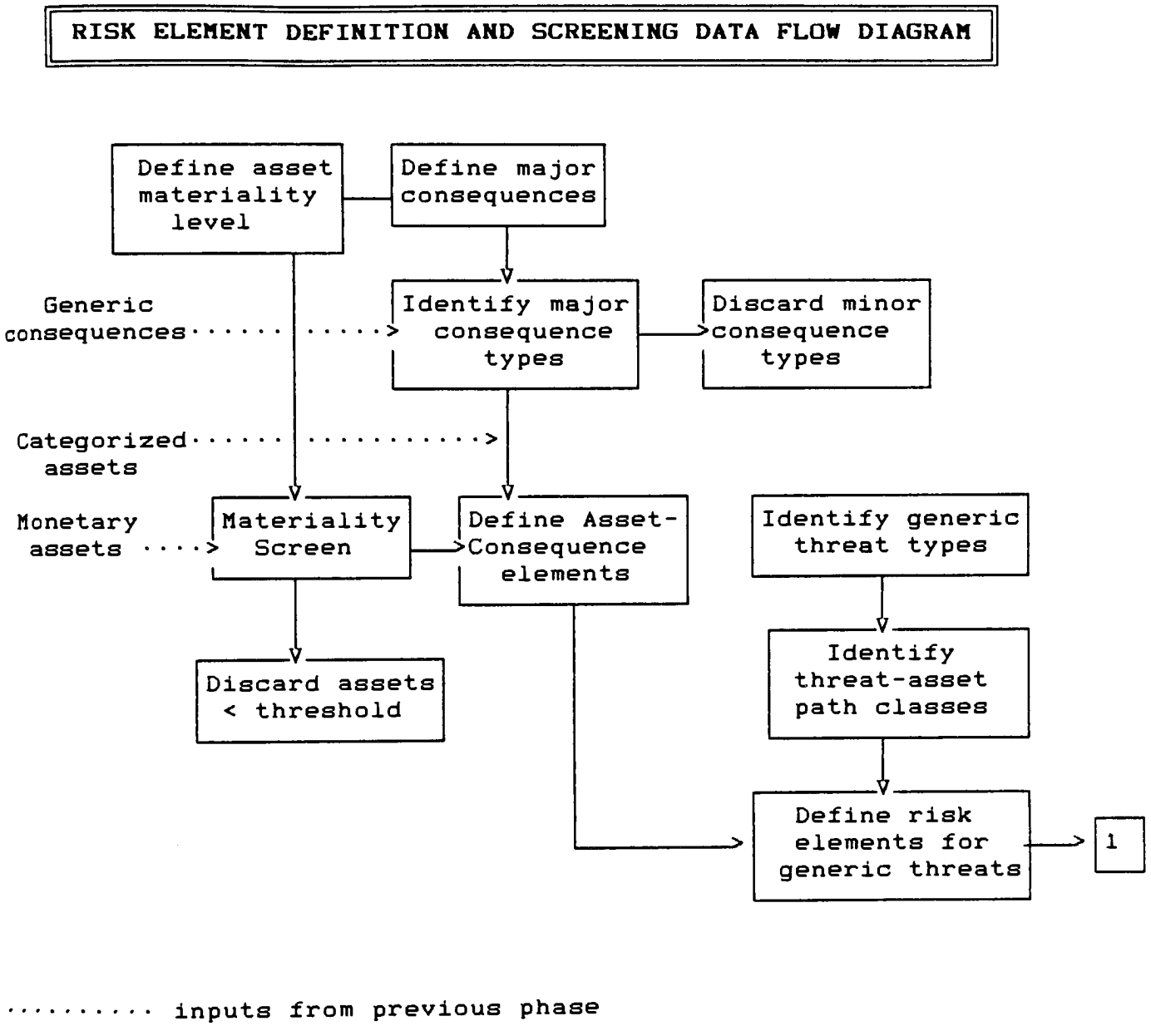



FIGURE 2A. Data flow diagram for risk element definition (REDS).

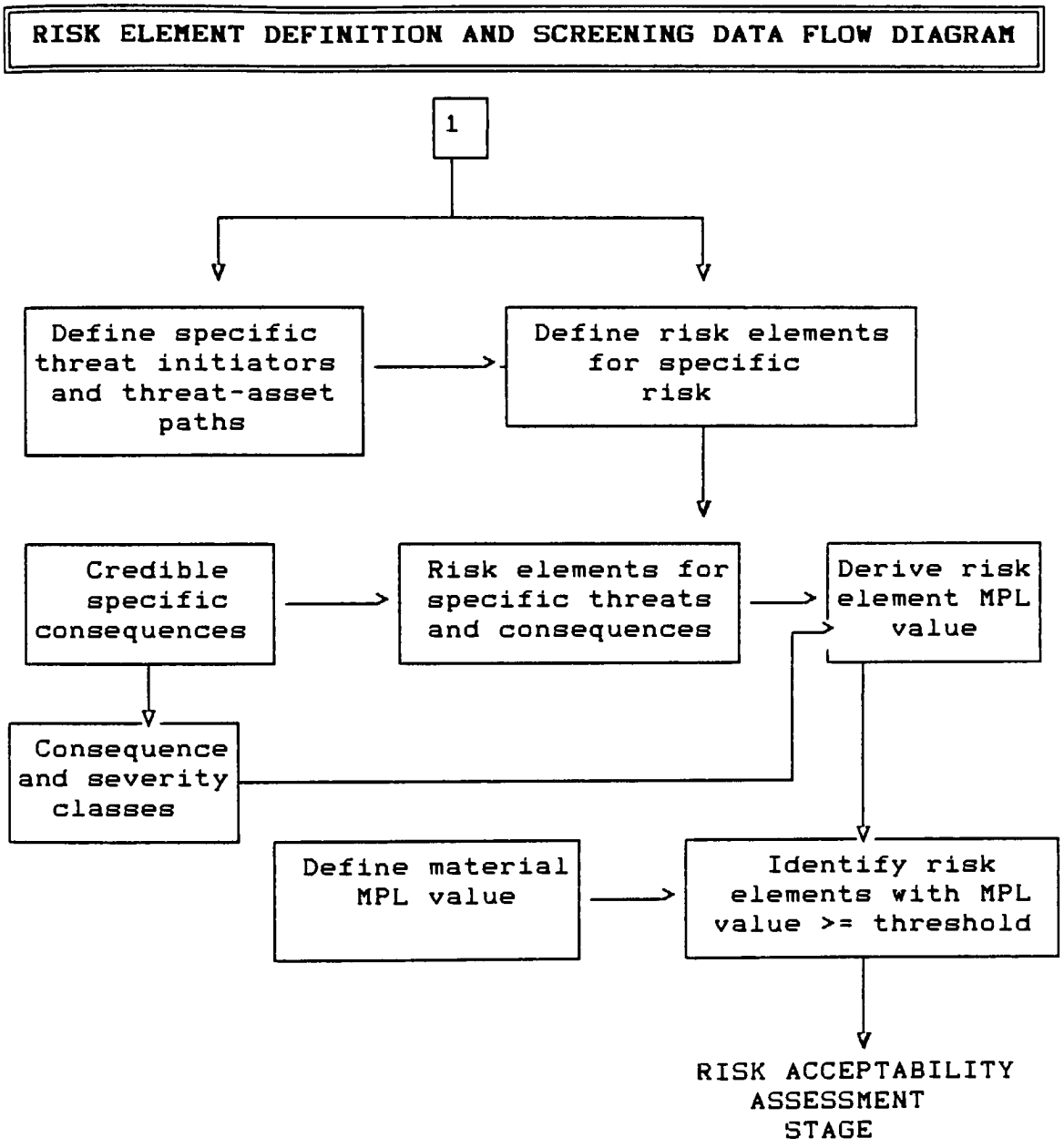



FIGURE 2B. Data flow diagram for risk element definition (REDS).

software asset and possible major consequences be: direct loss, denial of service, disclosure of data, or destruction of data. The formation of a generic risk element (GRE) is created from threat path /asset-consequence element. For example, human intentional via communication lines (threat-path) and alteration of data (asset-consequence) describes a GRE. Going from generic types to system specific categories provides the analyst with the initial structure for analyses, while being able to focus on one threat-asset path class at a time. To refine the previous example to a SRE, the analyst must look at the threat-path in GRE and identify all threat-paths within the generic definition. A specific threat-path could be that an unauthorized person using remote terminal gains access to database. Next the analyst looks at all possible specific consequences to that risk. Specific consequences may include production of erroneous data, piracy of software or total destruction of the database. Through this process, numerous combinations of assets, possible threats and their paths, and consequences lead to the formation of a variety of specific risk elements.

System security controls are placed in the threat-paths in an attempt to thwart or check the progress of the threat. In Figure 1, we see that preventative controls are placed between the threat and the assets and mitigative controls (detective and corrective) are placed along the path from assets to consequences. In case the preventative controls are

breached, mitigative controls attempt to contain and minimize losses.

Risk elements (RE) were now defined and the next step was to determine the maximum potential loss (MPL) for each RE. This was the fist level of risk element quantification. MPL assumes that there are no controls or the failure of all controls, in other words, the worst possible case. This is equal to the asset value assuming a single occurrence of the threat event: Risk = EF X PCF X MPL, where EF =1 (threat has occurred) and PCF = 1 (failure of all controls) and MPL represents loss value of consequences. It is used here to reduce the number of assets to be evaluated for potential damage. The inputs needed for each RE are: consequence value data, consequence value and severity class rankings, and equivalence severity classes. Severity class rankings help the analyst describe intangibles and other kinds of consequences that are difficult to describe directly in terms of dollars. Non-monetary loss evaluation was accomplished through the use of a semi-quantitative ranking scheme which was divided into six discrete sets of severity classes. At one end of the scale damage was considered light and inconsequential by management. At the other end of the scale, damage had wide-scale security implications. Coinciding with the non-monetary scale was an equivalent monetary scale, reflecting a range of monetary equivalent values for each set of non-monetary severity classes. The merging of the two class tables and their intersection gave the desired MPL severity

class number. MPL represents the total loss value associated with the loss or compromise of any particular asset. The severity class criteria are agreed upon through discussions with management.

In risk analysis, fine precision is not one of the prime requirements. It is accepted practice that an analyst must make some quantification judgements on an order of magnitude basis. If you can discriminate between 10,000 and 100,000, chances are that your analysis will be accurate. Another screening process at the end of the REDS stage eliminates those risk elements whose MPL value is less than the threshold materiality level. This threshold materiality level is usually defined by management. The purpose of this screen is to remove from the analysis any REs that cannot cause a single loss of significant severity.

The last stage in the Risk Analysis Phase and the last in my application was the Risk Acceptability Assessment stage. This stage resulted in the identification of those REs that were found to have the potential to produce unacceptable consequences. New controls or upgrades would be necessary and a new acceptability assessment made if they are not acceptable. First current control data was collected and a table was constructed to reflect the relationships between current controls and each RE. Control failure data (PCF) is also gathered. Subjective judgement, order of magnitude values, are used. Controls were sorted into two broad categories, either preventative or mitigative, reflecting the

controls' intent to deter, detect, prevent, recover from or correct threat situations. A loss potential indicator (LPI) is used as a parameter for evaluation of risk acceptability and informs us whether the current controls are adequate. LPI is the product of the probability of control failure (PCF) and the maximum potential loss (MPL). LPI represents the second level of quantification of the RE and is used to determine the acceptability of various risk elements. The LPI parameter reflects risk in the form of average loss one can expect to incur given the threat has materialized. It takes in account the reduction effect that the presence of controls have on the MPL. The derived LPI for each RE is compared against an acceptable LPI value. If it is greater than the proposed LPI threshold, the RE is an unacceptable risk. The threshold of acceptability is generally higher than the level of materiality.

At this point, the analysis revealed the risk elements that were unacceptable risks. Any RE with an apparent adequate level of security was screened from the analysis at this point. Further consideration for new controls or upgrading of present controls is needed to make the RE acceptable. Risk elements that were acceptable with present controls in place have been identified and any unacceptable risk elements were identified.

CASE STUDY. The first constraint placed on the risk assessment is as follows: individually, the physical

environment, personnel and administrative security policies, emergency/disaster planning and recovery policies are outside of the scope of this paper. For example, support systems such as power supply, air conditioning, or heating are not within the scope of the project. Normally, a risk assessment of these areas would be performed for completeness. It is important for management to acknowledge that these are important elements in any risk analysis. Management needs to know, for example, whether or not a system is vulnerable from members of its own staff. It is impossible to prevent an authorized user from abusing privileges, but steps can be taken to mitigate the damage and ensure detection.

The case study system to be considered is a VAX/VMS cluster environment. (See Figure 3.) The VAX cluster contains two processors, a VAX 8820 and a VAX 8550. All are booted from one system pack. The advantage lays in decreased complexity in updates and the existence of a common directory for operations. However, a disadvantage is, if a system disk fails, all systems fail. Another disadvantage is the increased probability of a system I/O bottleneck[52].

Mass storage servers known as Hierarchical Storage Controllers (HSCs) are connected to the processors by a star coupler. A star coupler is a passive device which can accommodate up to 24 nodes[53]. Nodes in the cluster can be a VAX or a HSC. The HSC70 can support a maximum of 32 tape and

52 Digital Equipment Corporation, VAX/VMS SOFTWARE, 1985.
53 Malamud, Carl, DEC Networks and Architectures, McGraw-Hill Book Co., N.Y., 1989, p.99.

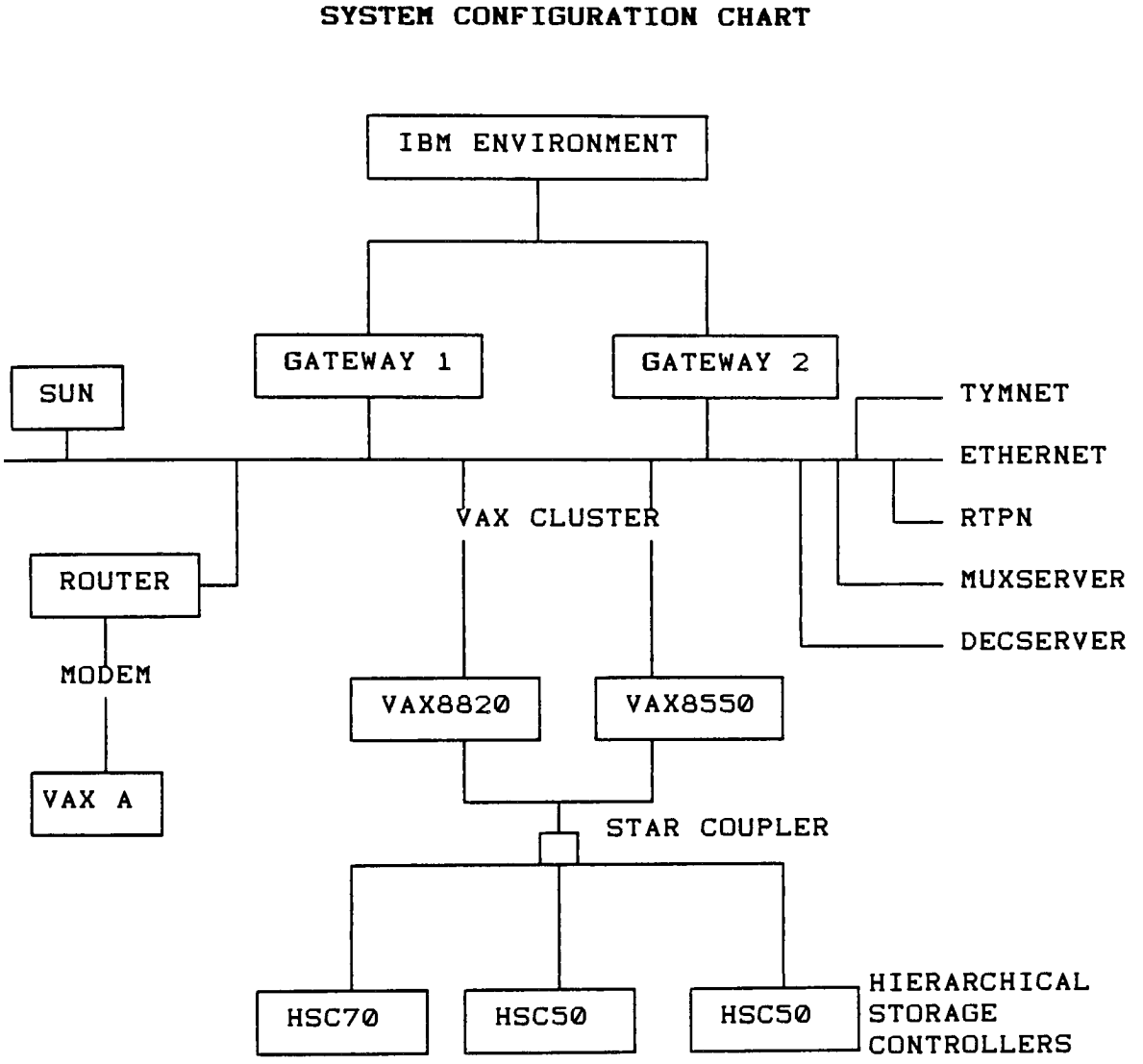



FIGURE 3. Case study system

disk drives while the HSC50 has a total drive connectivity of 24. The HSCs in this system provide a total of 10 tape drives and 80 disk drives to the homogeneous cluster. The star coupler itself has built-in redundancy enabling communications which will occur even if one of the internal transformers fail. The computer interconnect (CI) supports three kinds of data transfers: datagrams (DECnet), sequenced messages (VMS short messages) and block data transfers (data movement between cluster nodes).

A SUN workstation, dedicated to a specific application, massages data before it is downloaded to the VAX 8820. The information is then forwarded to another system. VAX A (2 microcomputers), used primarily for research and development programs, is connected via modems to the main system. At the moment, there is a console operator for this system with plans in the future to incorporate a cluster console for all existing system clusters.

The processing environment, once decentralized and now in a state of flux, is moving towards centralized clusters of processors and mass storage devices. The motivation is one of increased productivity and the capacity to better handle workload placement and customer requirements. The system includes a large number of office and personal computers that are able to take advantage of the high performance computer hardware in the central data processing cluster. Clustering will enable the organization to provide computer resources and applications cost effectively to the entire organization as

well as individual users. DEC/VAX representatives and an on-site organization provide support to operations, hardware, software and network problem management and resolution. Maintenance contracts guarantee a response time of 2 hours.

The primary mission of the system is to provide an end-user environment for decision support. A strategic marketing database, in-house applications, and a wide range of database and information retrieval software provide a multi-user group with the capability of ad hoc queries, the creation of databases based on customer requirements, good response times and the timely delivery of such information. Currently, the system averages 25 concurrent users with a projected 150 in the near future.

A relational database management package, ORACLE, provides for query reporting. The database is updated interactively from remote locations and additional information by monthly and quarterly tape feeds from other systems. It provides a wide variety of programs to the end-user. There is an on-going program to standardize operations for all groups involved in the information database. This would assist in database maintenance, detection of data duplication and ease the strain on limited resources. Standardization of documentation procedures offered via a software package of documentation tools is also in the offing. User education featuring training programs and classes in ORACLE and DEC/VAX instructions are offered in-house.

The environment is largely an interactive one connected by an extensive and varied network system. Access is allowed through multiple asynchronous networks, as well as by a high speed local area network, ETHERNET, which is characterized as a backbone configuration. This permits DECnet using the ETHERNET connection to connect to other DECnet nodes in the LAN[54]. Refer to the System Configuration Chart, Figure 3. There exist two gateways allowing communication from the DEC environment to an IBM environment and vise versa. Gateway 1, an experimental prototype, allows interactive communication from the IBM environment to the DEC world. Gateway 2 is used primarily for communication from the DEC environment to the IBM world. A value-added network, TYMNET, adds 32 lines used for the APL, Honeywell and IBM environments. Another asynchronous network, RTPN, services users in the local area with both hardware and software provided by the local telephone company. Server 1 supports 24 additional dial-in lines. A concentrator, Server 2, allows multiple phone lines via modems and RS232 connections for remote site access. Dial-in access is available through three lead numbers and hunt groups. The main concern of network personnel seems to be the lack of alternate paths and connectivity of divergent technologies present throughout the system. The case of multiple entry points and a large number of interactions with the system make adequate troubleshooting and diagnostics difficult.

---

54 Digital Equipment Corporation, VAX/VMS SOFTWARE, 1985.

Most of the security functions needed for data integrity as well as logging and monitoring operations are provided by the operating system itself, VMS 5.0. The primary form of authentication is password-based. A two step entry process is used with one password needed for DECnet access and another for entry into an ORACLE account. ORACLE sets privileges and restrictions at the application level. Some limitations are hardcoded within applications. User IDs are created by an Automated Account Management system. Turn around time for creation is two working days. There are assigned group administrators for creation control and deletion procedures for retired accounts. There is also a periodic password change program and periodic clean-up of inactive accounts.

## VIII. METHODOLOGY OF STUDY

STUDY ORGANIZATION. In order to analyze the applicability and value of the LRAM methodology, it was necessary to conduct a test case security analysis of a local system. The problem of locating a system for such an analysis was in itself very difficult and problematic. One organization appeared enthusiastic about the risk assessment project throughout the scoping process and interested in the application of a risk assessment methodology. The scope was defined and the value-added benefits were presented to the organization's top management. Unfortunately, at the end of the scoping process, it was decided that the exposure for such an undertaking outweighed the benefits of participation. The major reason given for denying access to the system was the fact it was a thesis project and subject to publication. No arguments could be delivered to sway the organization's viewpoint. This was disappointing, but it highlighted a problem with this area of research. There exists a general lack of cooperation and understanding needed for all to profit by the development of secure network environments. Eventually, a commercial system was located and authorization for the project was granted before any work on the project took place.

Some problems were encountered as the project progressed. Most significant were the vacillation of the level of commitment and enthusiasm for the project, the ensuing long periods of individual accessibility and the limited access to printed documentation. Originally, all contacts were made

through a liaison which made coordination of project objectives difficult. Every interview was documented and all information was substantiated through the corroboration of other staff members and/or available documentation. Several interviewees seemed to fear unfavorable retaliations and hence gave glowing reviews of their particular area. This information was soon verified or discarded through corroboration. Generally, whenever a difficulty or lack of cooperation was experienced, top management support would intervene to obtain the necessary participation and cooperation of the staff.

There was support by senior and middle management but very little, if any, publicity surrounding the project. At one point during the assessment, no contacts or queries were permitted while an internal audit was performed. Some ensuing secrecy and sensitivity remained after a two month lock-out. One must be able to communicate the requirements to top management and exhibit good interviewing skills. Everyone has different priorities, and as an outsider, others must be convinced of your motives.

The availability and access to sensitive and propietary data during the project presented another problem area. Many times it meant reauthorization from management which incurred major time delays. Regular progress reports kept management informed of the project status and communicated any problems encountered.

DATA GATHERING. To focus on the areas to be covered in the case study, a tour of the facility was completed at the early stages of the analysis. Data was collected primarily by interviewing persons directly involved with the case study system, software vendors, hardware service personnel, security personnel, and other supporting staff personnel. Several managers were consulted during the classification of assets. This was due to the broad scope of the analysis and to organizational divisions crossed by the target system.

Several meetings with management were necessary to determine the global goals of the organization, to develop an overview of company security policies, and to determine the threshold values to be utilized in the analysis.

Another method of data collection was the use of questionnaires and surveys. Some of the surveys administered consisted of statements of the existence of desirable system security attributes. Respondents were asked to check the BEST answers based on first hand experience and knowledge. The answers ranged from agree to don't know. These were assigned discrete values and, in this way, subjective opinions of the evaluators were quantified. All of the evaluators' answers were averaged on each question, thereby providing the basis for a statistical evaluation. Averaged scores were compared against expert opinion to aid in establishing the reasonableness of the answers and to quickly identify potential problem areas. Security issues involving the software development procedures, operation procedures,

specific application requirements, media controls and storage, backups and recovery procedures, network and user policies were developed using a combination of personal interviews and survey responses. Questionnaires were also used as an aid during the interview process and the development of scenarios.

Probability of Control Failure rates were established using surveys, interviews, system generated reports, vendor information, maintenance reports and expert opinion. Because of limited or imperfect historical data, inferential or inductive statistics was used to arrive at conclusions about the current controls. Generally, this involved drawing a set of conclusions about a specific control based on values observed in a survey. From this information one can derive the quantitative information to be used in the model-building process. Subjective estimates are often criticized for being derived from data and probabilities which frequently do not have an empirical basis. The task of determining exact values for model parameters, due to inconvenience, impracticality and availability of data, is a real issue. Additionally, the reluctance of management or vendor representatives to divulge specific information compounds the task. What becomes important is the auditor's base of knowledge, skill and expertise.

In the case study, most of the objective data was collected from computer generated event logs, maintenance reports and other system logging reports. A satisfactory risk monitoring system can provide the necessary input information

for the risk assessment. Inadequate or a lack of risk monitoring procedures prevent access to details of risk occurrences and subsequent losses. Sometimes the usefulness of existing monitoring reports were handicapped by containing either too little or too much information. This made it difficult to obtain pertinent information and made data comparisons from various sources to quantify amounts cumbersome or impossible.

The checklist approach was another tool used by the methodology. As a reference, it was very helpful in brain storming, however if relied on too heavily it can limit one's observations or distract the analyst from significant issues. Similarly, relying too heavily on system generated reports can also skew the analyst view of potential security risks. Potential exposures may not be audited or recognized by the staff. Either can cause one to overlook a serious vulnerability.

## IX. OBSERVATIONS AND COMMENTS

CONCLUSIONS AND RESULTS OF STUDY. The following criteria were employed in the Risk Acceptability stage (in the development of risk scenarios, also referred to as threat events, for the case study. The LPI threshold was defined at one. This meant that unacceptable risk threats were defined with an expected loss value per single occurrence of greater than $50,000. Previously, the MPL screen eliminated 33% of the threat events. These events were calculated at less than or equal to the MPL threshold of $50,000. Remember that at the MPL screen it is assumed that all applicable controls have failed. This equates to the formula: MPL = 1 (Expected Frequency of Threat) * 1 (Control Set Failure Rate) * asset value. FIGURE 4 represents the potential loss for the risk elements remaining in the Risk Acceptability stage. The loss is based on dollar estimates.

One of the high risk activities that proved to be unacceptable involved the bypassing of security controls and provisions to expedite problem solving and maintenance problems, compromising mainframe and microcomputer integrity. Surveys indicated that this method of trouble-shooting was employed nearly 40% of the time. The most expedient problem resolution was accepted without considering the corresponding level of risk. Generally, accountability and responsibility for poor fixes was non-existent.

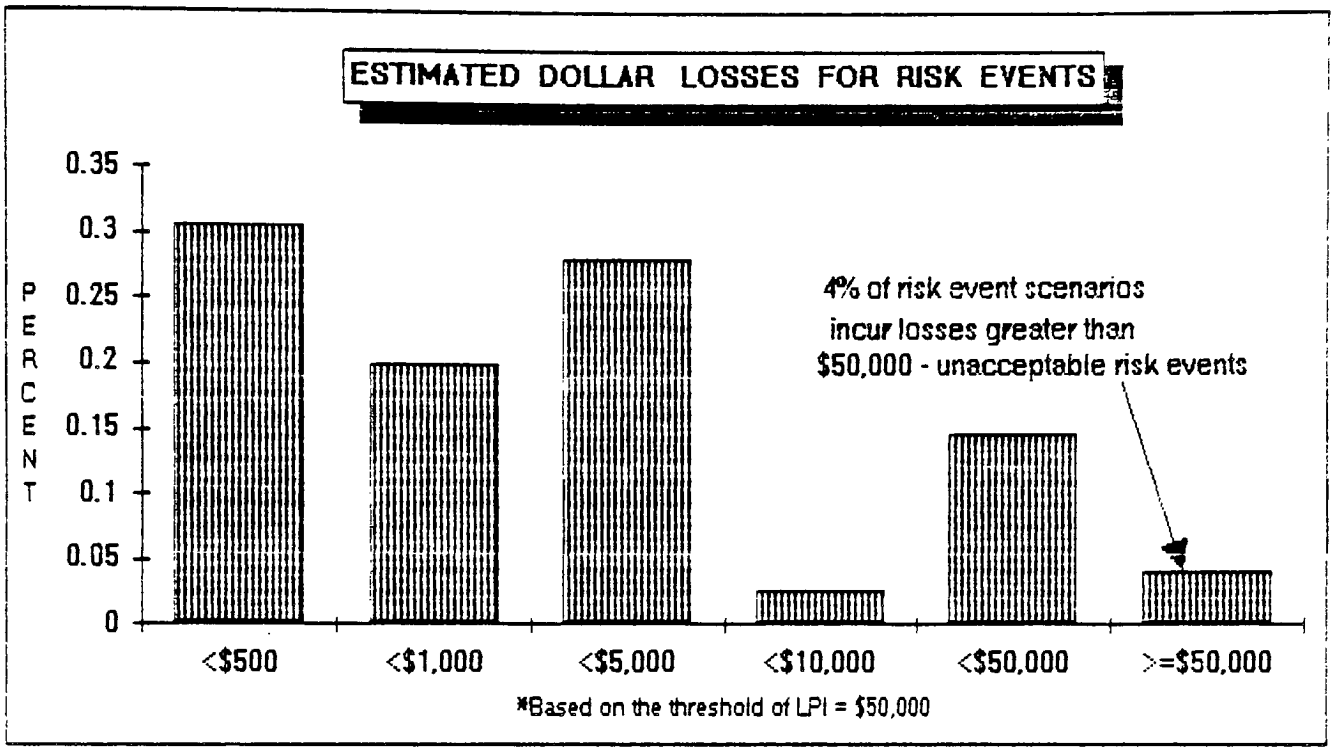



FIGURE 4. Case study results of risk events.

Another high risk activity and unacceptable risk event involved the lack of supervision for contract, vendor and service personnel. Supervisory control failure in sensitive areas would potentially occur 75% of the time. The assumption cannot be made that all contract, vendor and service personnel are honest and trustworthy. Unauthorized use of a protocol analyzer leading to the disclosure of sensitive information to outside individuals and the subsequent loss of revenue to the company is a serious consequence. As the speed of networks

approaches the speed of computing, the time required to compromise a network diminishes.

The lack of network management tools and the ensuing diversity of technologies exacerbated this particular threat. Maintenance and trouble-shooting arenas benefit from development of this capability or suffer from the lack of it. One must adopt a user's perspective and a total systems approach. The availability of status information and the development of a historical database for problem resolution is required to permit an integrated network management system to function. The current generation of integrated network management tools is beginning to provide an integrated approach to fault, configuration, accounting, performance and security management. Given these capabilities, network operations staff will be able to respond to and resolve network performance issues such as component or facility failures, poor response time and network congestion.

Unacceptable risk events comprised 4% of the total number of risk events evaluated. The overall security level of the case study appears to be acceptable. From surveys conducted, the personnel felt that the level of security in the case study system was average. The following chart (Figure 5) depicts the actual response. Sixty-five percent of the staff viewed the case system as possessing an average level of security. There were as many inadequate as superior and excellent responses. It is interesting to note that the majority of above average responses were received from less

tenured employees and below average responses were received from long term employees. It is questionable to endeavor to evaluate such a value though it may serve to confirm that improvements can be made and support the general findings of the model.

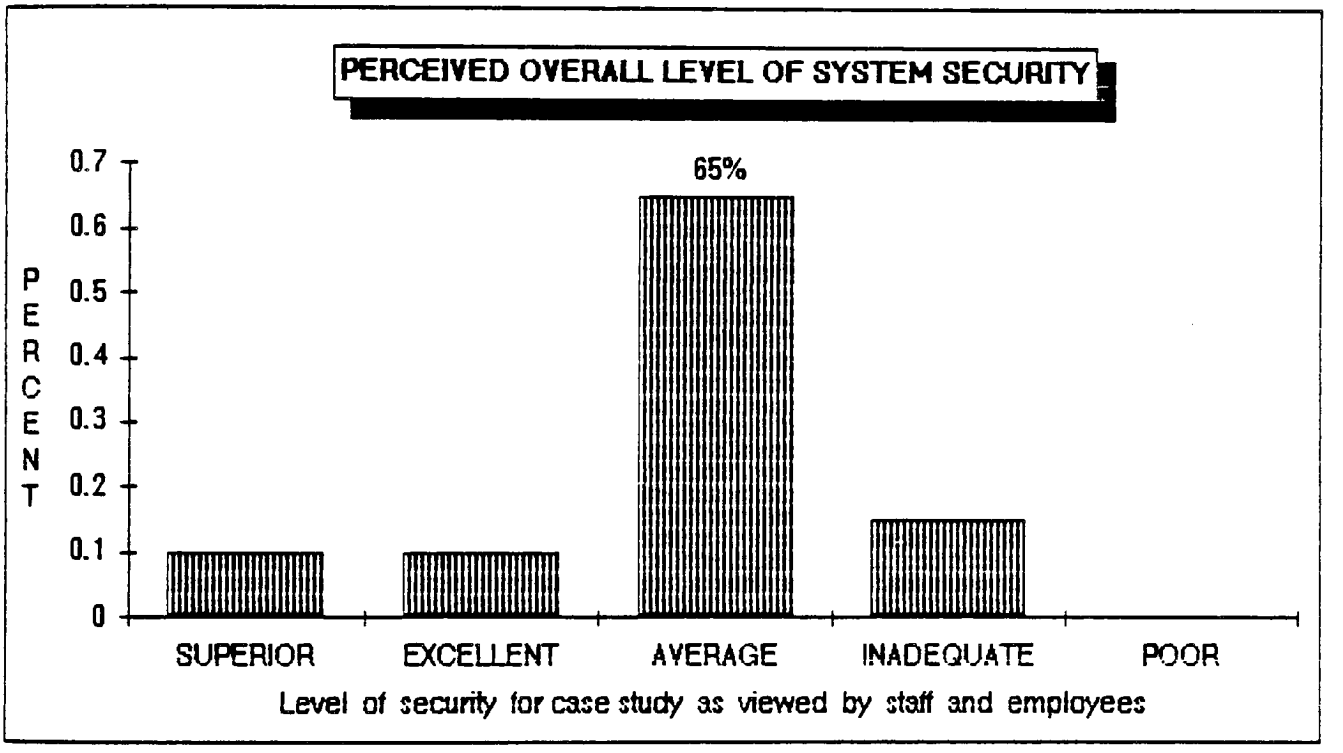


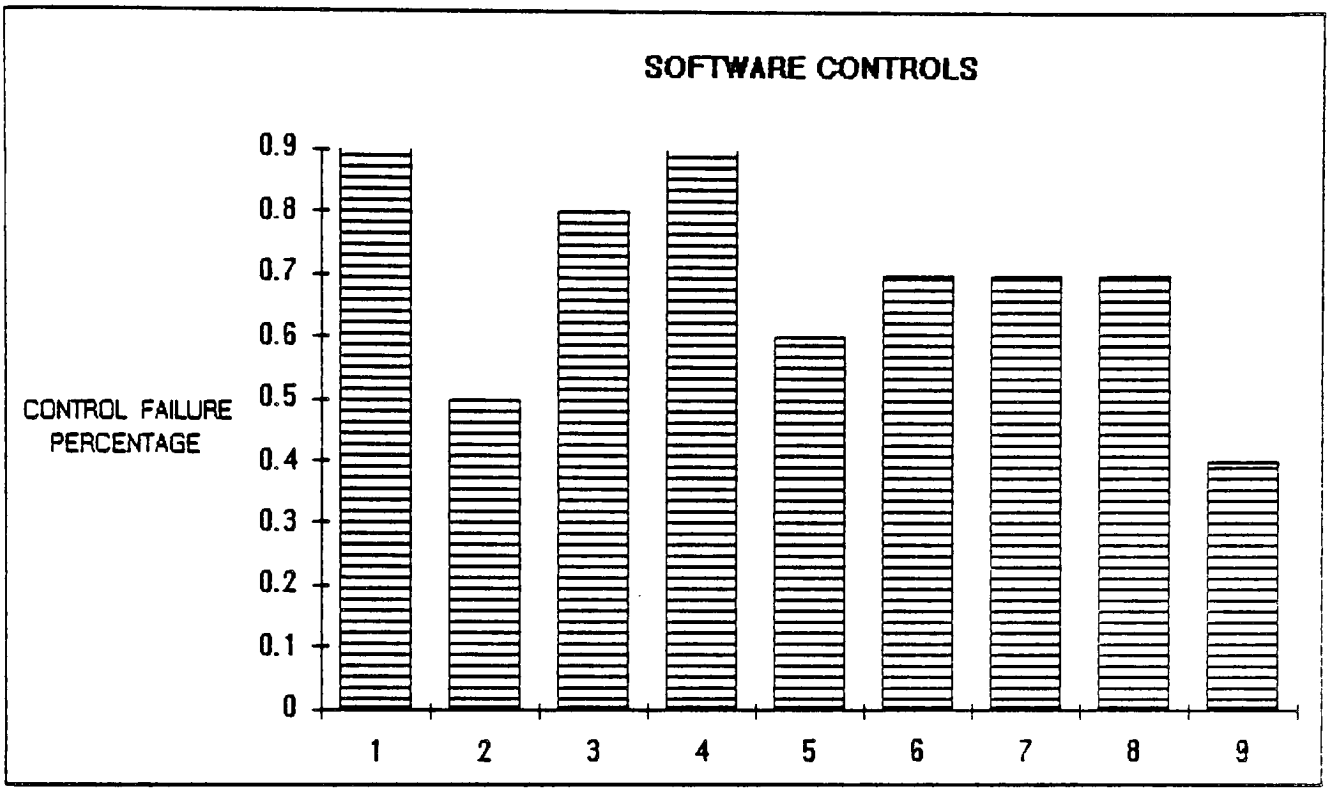

FIGURE 5. Perceived view of the overall level of security for the case study system.

The following risk events pose a substantial potential loss in the range of $20,000 to $30,000. The largest potential loss involved the inadequacy of change controls for software applications. Both production, decision support and system applications were at risk from the potential

unauthorized insertion of new program modules, modification or the deletion of existing programs. Accountability for modifications is necessary for the maintainability and reliability of the software. Corrections and enhancements to software should receive as much attention as the original development. There existed minimal stress testing, quality assurance before implementation or testing for functional correctness. The general lack of controls governing the software development and support processes did not impact the results as expected. It was expected that software errors and potential disclosure of information would produce higher exposures. A variety of risk scenarios involving software errors produced exposures in the $10,000 to $15,000 range. The opportunity for programmers and other personnel to exploit software and additional sensitive data is evident in the following chart (Figure 6).

The potential risk for information disclosure appears to be very high due to inadequate software controls. Personnel are not required to dispose of program copies and duplicate project materials in any controlled manner. Inadequate disposal of sensitive, obsolete or outdated information wasviewed to be a problem throughout the organization. Another organizational exposure was the inadequacy of system documentation. Duties and responsibilities of personnel system-wide were found to be impacted by documentation that at times was not available, accurate or well-maintained. There are several reasons why inadequate software controls are not

FIGURE 6. Probability of software control failure for the case study system.



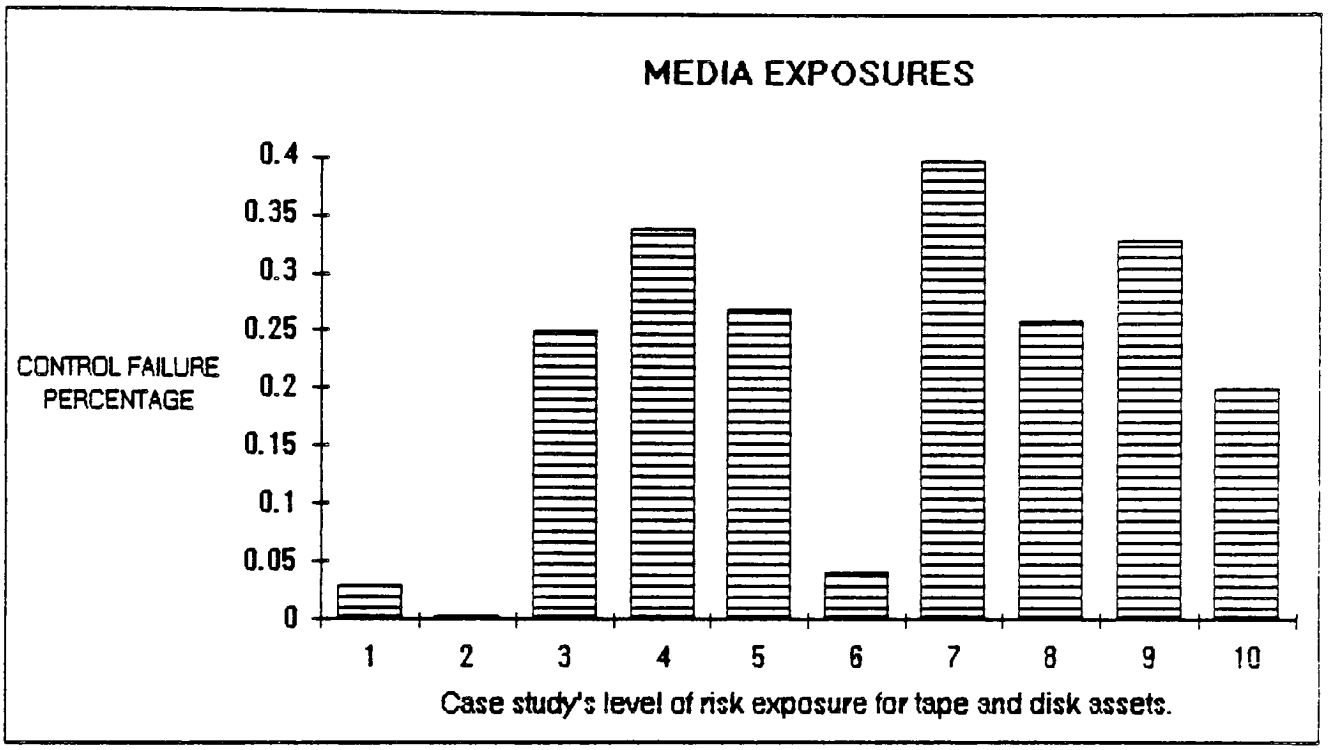

KEY:

1 Structured walkthroughs mandatory for program development.
2 Separation of test and production environments.
3 Programmers receive only the tools essential for task
4 All program copies, test data, and related project materials are required to be transferred to an authorized person on project completion for disposal.
5 A policy of testing and quality assurance reviews exists for all new programs.
6 There exists a verifiable record of each change made to the source code, who made it and who authorized the change.
7 Strict access controls on software tools.
8 Well maintained, detailed documentation for all applications.
9 Restricted access to program library and production data.

supported as a significant risk by the model. The presence of vendor supplied software and maintenance contracts for many of the software investments mitigates the impact of loss for many scenarios. A valid picture of software security may not have been studied since all program failures may not have been logged and reviewed. The combination of other controls in series or parallel reduce the impact of the evident lack of controls. Finally, the Loss Potential Indicator threshold was defined to be one. Even though only potential losses of greater than $50,000 dollars are deemed unacceptable, software development and maintenance is clearly an area where significant risks exist.

Acceptable losses located in the range of $15,000 to $20,000 include the threat of inadequate media controls. It is interesting to note the level of media exposures (Figure 7) within the computer operations area. Though the area was physically secure, these potential risks were seen to impact operations and availability of service to the users. Forty percent of the time, the movement of media was not recorded. Subsequent audits could identify the absence of tape media but could not mitigate the loss of processing time when unavailable. Other exposures revealed problems with everyday housekeeping and safety controls. Most of the current risks could be eliminated through the implementation of an automated tape management system.

FIGURE 7. Potential media exposures for the case study system; PCF's are represented for each control.



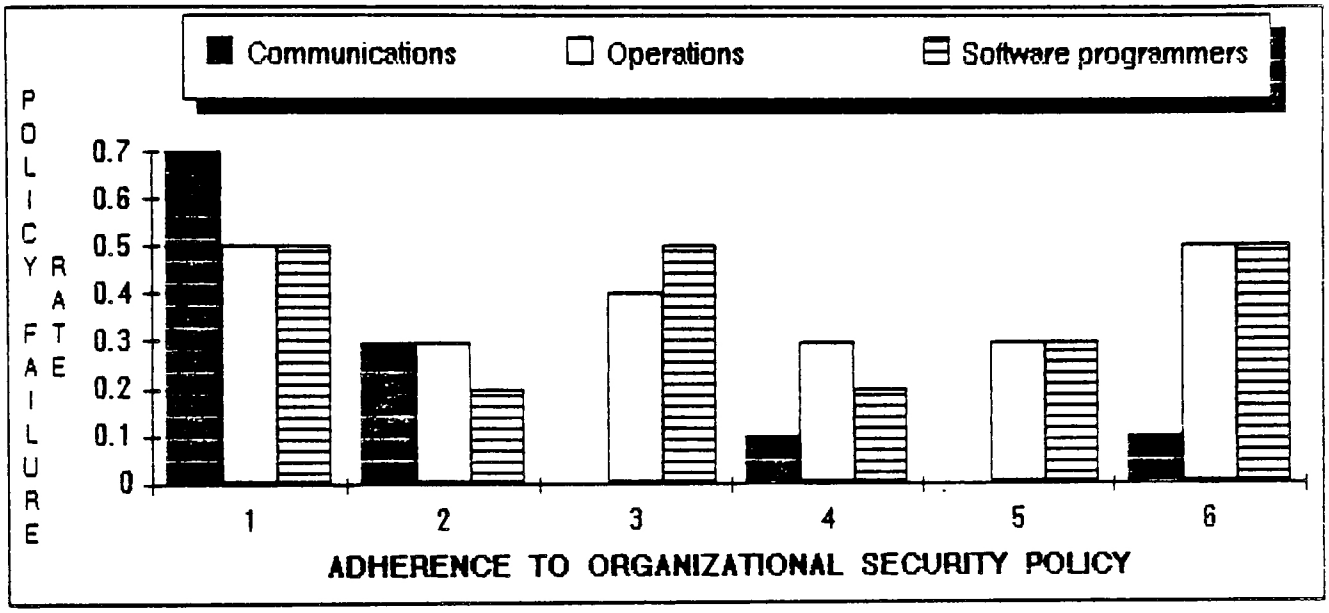

KEY:

1 All media is correctly labeled.
2 Backups are correctly labeled.
3 Cleaning of media is done periodically.
4 A cart or a tray is used to transport media.
5 Adequate disposal of sensitive, obsolete or outdated media (includes computer printouts).
6 Careful handling of backup tapes during recovery process.
7 The movement of all tapes and disks is recorded.
8 Loading of software onto the system is restricted and controlled.
9 Sufficient enforcement of media logging procedures.
10 Media left in secure area.

To set definitive management goals in the area of information security is imperative, however, successful achievement of those goals is dependent upon widespread knowledge of the program and compliance with security policies. The following chart (Figure 8) summarizes the effectiveness of six organizational security policies. The responses are separated into three general divisions: communications personnel, operations personnel and software programmers and analysts. The responses proved to be uniform across organizational divisions. The probability of failure for each policy is given by percent.

The chart establishes that on the average over fifty percent of the time personnel were not sure what the organization's security policies encompass. Security violations were not reported and accountability for security was not clearly assigned. The research did show that the least tenured employees commanded a higher security awareness. Perhaps, the indoctrination of information security policies at hiring was improving. The initial scoping of the organizational security policies and classification of information programs resulted in a positive impression. However, further research revealed that many of the employees were totally unaware of this comprehensive program. Poor management and employee communications can produce or increase information security problems.

FIGURE 8. Effectiveness of security policies and programs; PCF's are represented for each control.




KEY:
1 Security policies are clearly established and understood.
2 Security compliance reviews occur on a regular basis.
3 Security violations are reported to management.
4 Training of personnel on security procedures is adequate.
5 Personal knowledge of his/her security coordinator.
6 Responsibility for security is clearly assigned.

MODEL APPLICATION AND EVALUATION. If following the analysis, the analyst feels that the results are not reflective of his informal professional feelings, other system security techniques should be used. Perhaps the incidence of penetrations or the resulting damages are insufficient to build a case for a proposed security control. The author of

the methodology states that alternate techniques can give a higher degree of confidence that all existing vulnerabilities have been addressed. What might be missed in one approach may be noticed in another. In addition, employing several techniques can provide a cross-verification of results. Alternate techniques were not employed in the case study due to the stated scope of the project.

One merit of a good model is the capability of producing correct results with a reasonable amount of effort. It was felt that the LRAM model's development of risk profiles for each risk element produced useable results. It allowed for the future selection of control sets that maximize exposure reduction while staying within resource and other constraints. The risk assessment process is simplified through the use of a combination of objective and subjective criteria. The initial categorization of assets is based on the concept of making "criticality" assessments as well as value judgements. System and facility documentation served as the basis for the monetary valuations of assets. Those assets identified with a high asset monetary value or criticality to the system remained to be further analyzed. One effectively ranks the assets using these criteria. The criteria permit the modeling of all key factors necessary to evaluate the significance of any asset. Any redundancy factors present are accounted for at this step in the model-building process through the criticality assessment. Several assets were discounted at this stage due to low asset value and redundancy provisions

for critical function areas. Components that may cause an unacceptable downtime for any failure or compromise are also pinpointed. This information can be utilized later to the identify system components where fault tolerance may be a cost-effective reliability strategy. If downtime is not an issue, simply having redundant components on-site can provide reliability. Classified or sensitive characteristics completed the asset definition process. Sensitive or classified information was defined by the internal information classification system of the organization. This program is crucial for the proper protection of information assets. This assumes, of course, that the people understand the purpose of classification scheme and adhere to a clear set of guidelines in making these classification decisions.

The model's identification and inventory procedure for current assets was straightforward and efficient. Clustering the assets into related sets can be done and is a recommended practice to save the analyst time. In this way, the analyst will not have to estimate separate PCF values for each minutely defined systems asset. The level of definition for the case study was set at the major component level, such as CPU, application X, gateway and so on. To insure that all important assets were included, reviews of collected data were conducted with persons familiar with the system to corroborate findings.

The modeling process will suffer at the first screen, if the materiality level (asset value threshold) is set extremely low. In the case study, the Materiality Level was defined at $15,000. As with the other defined threshold levels (MPL and LPI), the effectiveness of the screening process will be diminished if set low. The analyst would be forced to carry large data sets into each progressive stage which is cumbersome and counterproductive. The analyst must guide management in setting these levels at a reasonable level but at a level that will still reflect management concerns. The risk assessment process involves a considerable amount of information, data and calculations. Any mechanisms that foster time-efficient use of the information gathered, while still retaining credible results, should be utilized. It was felt that all significant assets were carried forward in the analysis. However, a very large or complex system reduces the practicability of this kind of methodology unless it can be dissected into statistically independent subdivisions.

One inherent weakness of the LRAM approach is that its success is based directly on the capability of the analyst to identify the threats and vulnerabilities correctly. Several experts from management were asked to make judgements on the threats and vulnerabilities of the organization and system. An expert refers to someone with expert knowledge about the area for which the risk assessment is being conducted. To assist in the risk profile development, they chose the generic consequences that had the potential for inflicting the most

significant damage to the organization. The samples were pooled and evaluated. It was interesting to note, that very few differences existed among their opinions. This presented the analyst with a high level of reliability for the identification of generic risk elements. The resulting major consequences for the case study were identified as:

- Direct Hardware or Software Loss
- System Interruption and/or Degradation
- Disclosure of Information to Outside Organizations
- Disclosure of Information to Unauthorized Individuals
- Data and/or Software Alteration or Destruction
- Direct Impairment of Organizational Ability to Perform the Primary Mission
- Induced Diversion of Organizational Resources

Major consequences were then paired with assets to arrive at those elements which would become known as asset-consequence pairs. The asset list and major consequences defined the more basic question "What should constitute the results of the analysis?".

The pairing of assets and consequences was facilitated by the model's extensive use of matrices (Appendix I). The matrix was invaluable for the development of risk elements considering the large amount of data carried forward in the analysis. The matrices also allow the analyst to proceed in a very structured, orderly manner while providing a maintainable, flexible format for reference.

A brief digression is necessary to discuss the question of quantitative versus qualitative estimates. Reliability and usability of the model are embodied in this question. As mentioned, one goal of any risk assessment methodology is to

obtain useful and reliable results. Reasonable approximations that simplify the process must be acceptable. This is necessary due to the incompleteness of available data, the unpredictable nature of loss exposures, the lack of historical data and the attempt to quantify intangibles. The nature of computer abuse and unauthorized access is not a problem that easily lends itself to quantitative analysis. The composite effect of all of these factors leads opponents to criticize the quality of the results. Most say they are dubious at best and pure guesswork at the worst. Many of these same criticisms were voiced by participants in the analysis. The issue between quantitative and qualitative estimates becomes a moot point. Obviously, you want to make the estimate quantitative if possible.

Both the Maximum Potential Loss (MPL) and Loss Potential Indicator (LPI) parameters rely in some measure on the combination of objective and subjective data. The purpose of the risk analysis is to develop risk exposure information to be used as a basis for management action. Management can utilize this information to initiate security actions. They can subsequently reduce the exposure by reducing the impact effect (MPL) or they can reduce the potential loss (LPI) by protecting or dispersing assets subject to the loss. The importance of these parameters in the formal analysis and decision-making process cannot be discounted.

In defense of the LRAM model, analysts are encouraged to quantify the consequences whenever practicable because of

quantitative requirements in the later stages of the model. In the cost benefit stage, accurate dollar estimates of consequences require a quantitative estimate which are needed to give sufficient resolution to the cost-benefit assessment, prioritization and selection of proposed control sets. At this point in the methodology, qualitative estimates are meant to be a time-saving device without diminishing the risk elements' proper assessment. Equivalent dollar estimates in the later stages will be made on a reduced set of unacceptable risk elements. The probabilities and data used in the case study were as close to reality as possible, ensuring the better value of MPL and LPI parameters.

The subjective estimates for non-monetary losses used in attaining the MPL could be considered potentially affected by existing uncertainties. However, the equivalence criteria is a reflection of management input and one has the flexibility to utilize non-conservative or conservative estimates for the merged MPL value. The propensity of individuals to underestimate indirect losses and less apparent implications associated with the qualitative assessments of loss values was felt to be an issue. Hence, high-end estimates were utilized and conservative values were used in the merging of the MPL severity class tables. In this way, the probability of an underestimation of losses would be greatly diminished. While the severity class criteria is a coarser value analysis, a high level of confidence in the MPL remained because of the reasons previously stated.

A primary inherent weakness in the LRAM model involves application. This approach required an extensive study of the system and supporting organization in order to establish threats and consequences, to determine probabilities and to obtain cost figures. It demanded extensive surveys and interviews involving many people and was a time-consuming effort. Organizational divisions and compartmentalization forces the analyst to interview many people to obtain and corroborate data for one risk element. Admittedly, once a database is established for the model-building process, a significant time savings would be realized. The advantage to using software to conduct the risk assessment, in addition to time, is that a partial or complete assessment could be easily made again without repeating the entire process.

This leads us to an inherent weakness in any qualitative assessment. The risk assessment becomes indirectly based on the insights and past experiences of the personnel involved. Experts within an organization may unconsciously introduce a measure of institutional bias into the selections of threats, consequences and control failure probabilities. Yet, the model almost mandates that such a selection be made because of the knowledge and skills that they possess. The model is not perfect, since it is also subject to the failings of humans who cannot model every situation. But it is a viable tool that will identify significant risk events.

The development of the risk element (RE) and the Maximum Potential Loss parameters (MPL) cannot be based entirely on

objective data. The MPL is easily perceived as the summary of the costs of the threats with the occurrence of one threat event. It is the summation of direct and indirect monetary losses and indirect non-monetary losses. First, let's examine the kinds of losses it attempts to model. Some REs incur a direct monetary loss at the point of compromise and incur no other losses (Figure 9). In most instances, the minute a business loses an application, some loss occurs. This is independent of the duration of the loss. Another RE may incur an initial loss but also incurs costs directly related to the time duration of the compromise (Figure 10). For example, the loss of an application due to media corruption incurs initial recovery costs but also incurs cost related to the lack of availability dependent on its criticality. The loss of an inventory application may become critical after 24 hours or a production application may become critical within hours of compromise. Some REs will exhibit no initial direct losses but incur time-dependent costs immediately (Figure 11) or after some period of time (Figure 12). Opportunity costs, as in the loss of expected revenue can be considered part of the time-dependent costs. In addition to the duration of the loss, an application may exhibit a wide range of loss dependent on the time of day the compromise occurs. If the application is active only after 5:00pm, losing it in the evening would be significantly more expensive than in the morning. The last input affecting the losses, is the frequency of the RE. A greater impact may result if the losses occur repeatedly in a

short period of time than over an extended period of time, due to the increased pressure against limited resources.

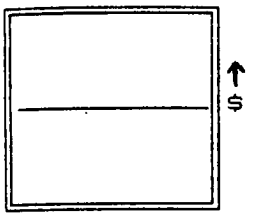



Figure 9

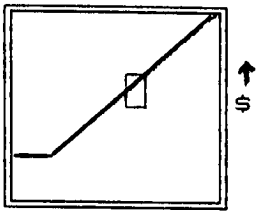



Figure 10

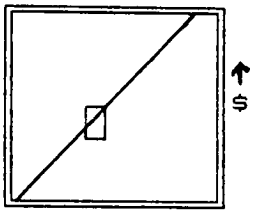



Figure 11

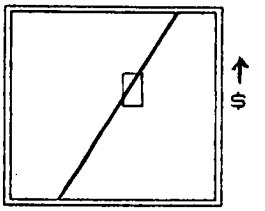



Figure 12

* □ denotes point of criticality

The only way the model can reflect the total range of time-dependent costs is through the specific formation of risk elements. For example, the specific risk element (SRE) will state that the duration of a particular risk event is 2 days, 1 week or whatever. The analyst would have to generate a multitude of SREs to accurately model one risk element. However, throughout the assessment the model has proposed using the worst case scenarios. The case study system was evaluated using the point of criticality for defining the MPL. For example, if the loss of an application becomes critical after 3 days, then that was considered to be the worst case scenario. This still does not account for the increasing impact of the loss if it continues to exist beyond the critical point. One can argue that this would not happen because management at this point would commit all available resources to prevent escalating costs. Only through documentation, will subsequent analysts know the point of criticality utilized to establish the MPL. This diminishes

but does not negate the repeatability claims of the methodology. It only makes comparisons more difficult in a changing environment. The fluctuations in frequency are not modeled. Instead, the LRAM formula incorporates the expected frequency of threat events based on occurrences per year.

The Loss Potential Indicator (LPI) of each risk element is the product of the Maximum Potential Loss (MPL) and the Probability of Control Failure (PCF). The probability of an event or set of events is a number between Ø and 1. If the event has the probability of Ø then its occurrence is impossible; if an event has the probability of 1 then its occurrence is certain. Finding this value between Ø and 1 which represents how likely an event is to occur is a fundamental part of most types of statistical analysis. The probability theory provides the foundation for the methods of this analysis.

The LRAM model involves the evaluations of just how likely it is that certain loss potentials will occur. Probabilities that are determined by the long-term frequency of an event can be referred to as objective probabilities, since they are based on objective evidence. Subjective probability assigns probabilities based on the analyst's subjective estimates using prior knowledge and experience as a guide. Proponents of a formal, quantitative method of risk analysis claim that better identification and quantification of potential security problems would lead to improved risk avoidance and risk management decisions. The problem with

this approach to estimating probabilities is that, in the real world, there may be little or no historical data available on which to base such an estimate. However, subjective probability can be determined. The rules and operations governing probability theory are the same whether the estimate is derived by an objective or subjective approach.

The first step in the LPI calculation, is to determine the relevant current controls and the corresponding Probability of Control Failure (PCF) rates for each RE. Aside from data collection problems, the rates can be viewed with a medium to high level of confidence. In the case study, anyone involved with the system was covered by surveys and response were received in total. There are several components to the LPI quantification process. The MPL, PCF, Consequence Reduction Factor (CRF) and the definition of mitigative and preventative control blocks. Because of the number of semi-quantitative estimates and the potential effect of compounding errors of judgement, this parameter was felt to be the most questionable. In order to quantify the fraction of times the controls fail to mitigate the effects of a threat on an asset, represented by PCF', an additional estimate is required. The Consequence Reduction Factor (CRF) represents the fraction of MPL for a specific risk element that will result when a mitigative control succeeds or functions properly. Thus, the formula for the PCF for a mitigative control is represented by PCF' = PCF X (1-PCF) CRF where CRF = Reduced MPL divided by

the non-reduced MPL[55]. The reduced MPL is arrived by a subjective estimate as to the mitigating value of the control on a specific consequence or loss. The extent a mitigating control reduces loss is an extremely dubious estimate. One way to attempt a quantification would be to examine the impact with and without the mitigation action which is impractical. In addition, some mitigating controls, such as a policy for punitive action, defies easy quantification. Because it was felt that CRF estimate is given under extreme uncertainty, the credibility of the estimates was questioned. A sensitivity study was conducted to reflect LPI's sensitivity to the changes in estimators (Refer to Appendix II). The results showed that errors in estimates falling at extreme ends, either nearly total mitigation or no mitigation, could affect the quantification of the LPI. The semi-quantitative LPI parameter was not sensitive to the CRF if moderate estimates were used. It was felt that the CRF estimates did not significantly impact the resulting LPI estimates, although essential to complete the modeling of the mitigating controls. The author recommends approximation of values throughout the LPI quantification process because of the semi-quantitative framework. It was recommended that PCFs be approximated to the closest estimate of 1/1000, 1/100, 1/10, 1/5, 1/2 or 1. CRFs should be approximated to the closest estimate of 0, 1/10, 1/4, 1/2, 3/4 and 1. However, it was felt that a better

55 Guarro, Sergio B. "Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management" and discussions with the author, Computers and Security, North-Holland Publishers, 1987, pp.493-504.

value was derived by using approximations only to arrive at the CER, especially since the later stages of the methodology were not applied. It was also felt that a higher level of quantification was desired by the organization. If point estimates for the MPL and PCF have been calculated, a point estimate for the LPI can be derived by applying the formula LPI = MPL X PCF(CER). The ability to fine tune the model at several entry points gives the analyst control of the level of quantification desired. At the end of mitigative and preventative control probability calculations, an approximate total value was then equated with an Control Effectiveness Rank (CER) for establishing a total Integrated Control Set (ICS) value. The resulting LPI value is a semi-quantitative value based on the equivalence criteria carried throughout the model-building process. The LPI and other significant model parameters are defined in general and graduated terms and the continuity of the MPL, MSC, NMSC and LPI ranges facilitates an understanding of intermediate and end results. Useful information condensed into a few summary parameters aids both comprehension and comparison of these measures. The severity class ranges also functioned as a check for reasonableness throughout the implementation of the model. If miscalculations were made during the model-building process, it would become apparent during the future stages of the model.

## X. SUMMARY

Risk management is a tool that attempts to maximize exposure reduction by assisting management in the selection of appropriate controls. Just as important, it guides the assimilation and integration of security policy practices and procedures into the normal process of everyday computer-based activities through periodic assessment. LRAM can be used effectively as long as its purpose and limitations are understood. It is a tool that serves as a complementary function to other security techniques.

The LRAM model shows considerable promise and great potential in the risk analysis and computer security field. Methodologies relying on precise metric and consensus techniques to substantiate their results produce volumes of data in the process. The work effort required is above what most organizations are will to expend for security-related decisions. The completeness problem, the ability to cover and model all possible types and combinations of threat events, has long been the Achilles' heel of risk analyses. Traditional checklist methodologies are prone to oversimplifications and generalizations which exacerbate the completeness problem. The approach tends to overlook many potential vulnerabilities. It is not comprehensive for all shapes, sizes and complexities of computer systems and difficult to tailor to any one environment. The LRAM approach is a blend of quantitative, semi-quantitative, and checklist methodologies. A stepwise evaluation leads from a semi-

quantitative framework to a quantitative framework for a reduced set of unacceptable risk events. The LRAM model is enhanced by utilizing different methodologies to its advantage.

The feasibility of employing LRAM risk assessment model was supported by the case study. It was necessary to reevaluate data and make refinements throughout the model-building process to arrive at the best available estimate of future losses and benefits of current controls. The criticism of excessive costs to perform an effective risk analysis is valid. The manual process can become an enormous task when many functions and control alternatives are considered. In the case study, delays caused by unresponsiveness or unavailability significantly increased the time required to complete the project. An internal team of dedicated personnel, with unlimited access and complete cooperation, could achieve timely results and meet the needs of the business environment. Though not obsolete, changes in the past year have made the results of the case study less useful. However, the identification of critical information elements and organizational security problems remained valuable. The case study provides a means for recommendations concerning security improvements. The scenario technique used by LRAM is a useful communication tool. Co-workers, management and staff members can easily comprehend the vulnerabilities that exist. Besides a time-savings, many benefits are derived from automating the risk assessment process. The computerized files increase the

availability of information necessary to perform future risk analyses. The cost reduction would be substantial, because voluminous calculations are performed by the computer and the number of staff needed for the project decreases. Finally, the report preparation costs would be substantially reduced because little manual intervention would be required. Risk assessment, while determining what risks are present in a given system, must be cost-effective.

Probability statistics, or decision-making under uncertainty, is commonly used in our daily lives. Many decisions are made without knowing the certainty of the consequences. A poor choice will cost us time and money, and sometimes place us at considerable risk. Using probability statistics as a decision-making tool, we can limit the risk of making decisions under uncertainty. The LRAM methodology, viewed in this light, is used as an aid by the decision maker. It helps decide what information is needed for a particular type of decision and how best this information can be collected and analyzed in a formal, structured process.

The flexibility of the model is achieved at the cost of requiring a person applying the model to be thoroughly familiar with the operation as well as the model-building process itself. The model requires one to be computer-literate and familiar with a significant amount of risk assessment knowledge in order to achieve the maximum potential from the model-building process. It is presented so that an individual familiar with both disciplines can easily

understand and apply it. The model is extremely versatile and an application of the model can answer a variety of questions. It can identify system assets, the MPL representing the maximum loss for a specific set of risk elements, the LPI representing effectiveness of current controls, cost-benefit information or answer any other question requiring an assessment.

Survey and questionnaire data supported several trends in computer crimes and systems abuse. If one believes that crime follows opportunity, the increase use of personal computers and workstations in business should also show an increase in computer oriented crimes for economical, personal and political reasons. The risk assessment findings supported that employees remain the primary source of threat to any system. Security of any information system depends heavily on employees and individual system users accepting and complying with good security practices. An organization must establish base information management requirements including information classification definitions. Employees must be educated and motivated to support security standards and policies. Intentional, unintentional or system induced security violations must be anticipated. People are the most important component of any loss prevention program and accountability becomes the enforcement mechanism that deters and detects security violations, system errors and omissions.

As a society, we are about to face the impact of the first generation of children who have grown up with computers.

This suggests a higher level of expertise and sophistication which can lead to potentially more serious computer offenses. Robert Morris has been recently convicted of unleashing a worm over a nationwide network. The maximum sentence could have been five years in prison and a $250,000 fine for the felony conviction. Many felt that Morris's sentence of 400 hours of community service, a $10,000 fine and a three year probation[56] was not a strong message to other would be pranksters. Society's vulnerability and dependability on computer networks merit a stern response to the Morris affair. The most celebrated computer abuse case in recent times has succeeded in increasing public security awareness, but has failed to send the signal that such acts will no longer be tolerated. Sanctions against perpetrators and the barring of offenders from sensitive positions in computing will help prevent computer crimes and deter future computer criminals.

---

56 PC WEEK, May 14, 1990.

INTERVIEW SHEET___ of___ date:

Interviewee:_____

Job Description/Expertise:_____

---

Information Processing Assets:

| Possible Material ASSETS | Related Concerns CONSEQUENCES |
|---|---|
| A1. | |
| A2. | |
| A3. | |
| A4. | |
| A5. | |
| A6. | |
| A7. | |
| A8. | |
| A10. | |
| A11. | |
| A12. | |
| A13. | |
| A14. | |
| A15. | |
| A16. | |
| A17. | |
| A18. | |
| A19. | |
| A20. | |

INTERVIEW SHEET___ of___ date:

Interviewee:_____

Job Description/Expertise:_____

---

Data Communications Assets:

| Possible Material ASSETS | Related Concerns CONSEQUENCES |
|---|---|
| A1. | |
| A2. | |
| A3. | |
| A4. | |
| A5. | |
| A6. | |
| A7. | |
| A8. | |
| A10. | |
| A11. | |
| A12. | |
| A13. | |
| A14. | |
| A15. | |
| A16. | |
| A17. | |
| A18. | |
| A19. | |
| A20. | |

**ASSET MATERIALITY DECISION TABLE**

Asset Materiality Threshold Value $.....K

| ASSET NAME | DIRECT LOSS VALUE$ | CLASSIFI-CATION (U,C,S) | CRITICAL (Y/N) | SENSITIVE (Y/N) | KEEP (Y/N) |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

CLASSIFICATION: Unclassified (U), Confidential (C), Secret (S)

COMMENTS:_____
_____
_____
_____

**MATERIAL ASSET-MAJOR CONSEQUENCE TABLE**

| | MAJOR CONSEQUENCES | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| MATERIAL ASSETS | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

C1-

C2-

C3-

C4-

C5-

C6-

C7-

C8-

COMMENTS:_____
_____
_____
_____
_____

RE WORKSHEET

ACCEPTABLE_____

RISK ELEMENT NUMBER:_____
ASSET/CONSEQUENCE:_____
THREAT/PATH:_____
DESCRIPTION:_____
_____
_____
_____

MONETARY LOSS:_____ MPL:_____ NMSC:_____
NON-MONETARY LOSS:_____ LPI:_____ MSC:_____

| AFFECTED ASSETS | Consequences | CRF |
|---|---|---|
| SPECIFIC POTENTIAL CONSEQUENCE DESCRIPTION | | |

CER:_____

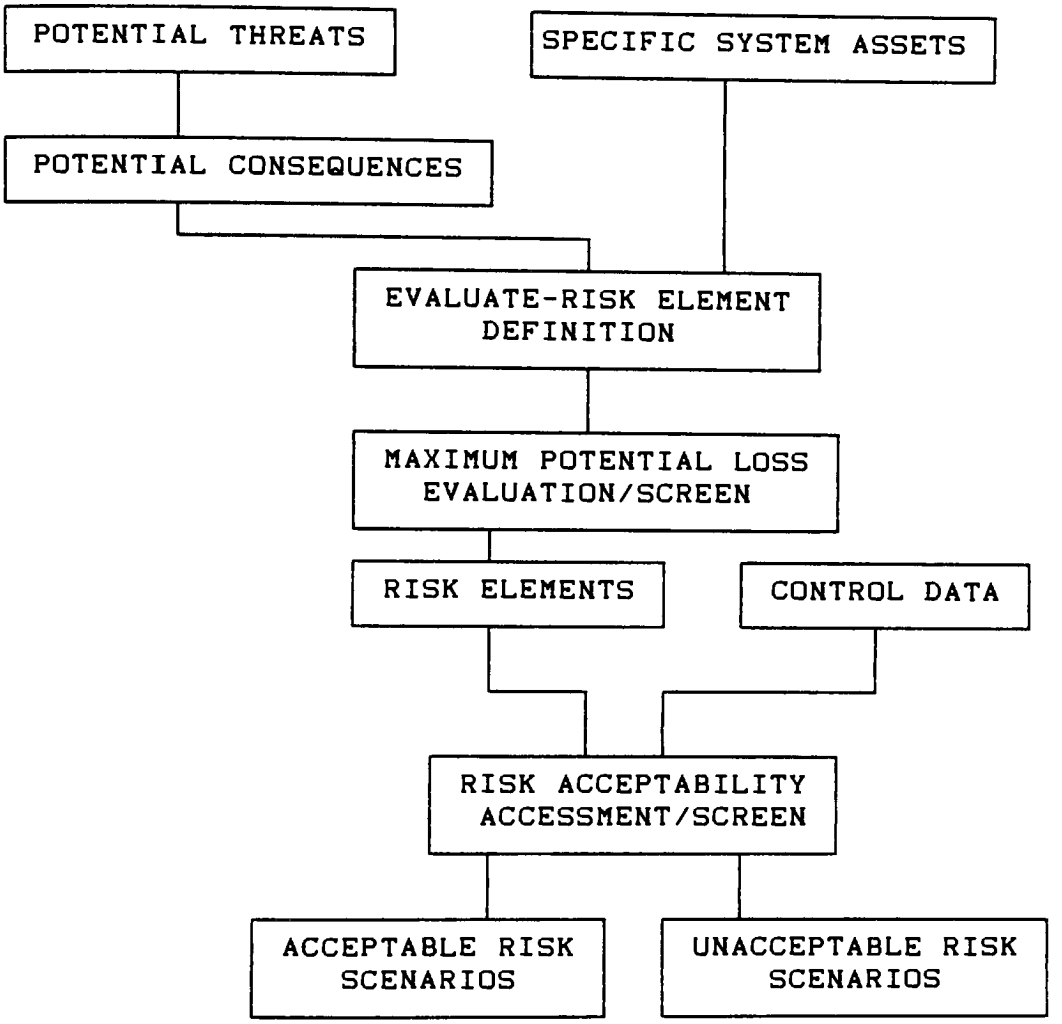
CURRENT CONTROLS
PREVENTATIVE: PCF

MITIGATIVE: PCF'= PCF + (1 - PCF) CRF

# APPENDIX II

Case Study Documentation

**COMPUTER SYSTEM RISK ASSESSMENT**
BASIC STEPS



## GENERIC CONSEQUENCES

Check the consequences you consider important or major.

- ☐ Direct hardware loss (ie. repair time or replacement)
- ☐ Direct financial loss (ie. diversion or theft of funds)
- ☐ System Interruption or Degradation
- ☐ Disclosure of information to outside organizations
- ☐ Disclosure of information to unauthorized individuals
- ☐ Theft of equipment or service by outside organizations
- ☐ Theft of equipment or service by unauthorized individuals
- ☐ Classification regulation violation
- ☐ Readily detectable data and/or software alteration or destruction
- ☐ Undetectable data and/or software alteration or destruction
- ☐ Organizational embarassment
- ☐ Induced diversion of organization resources (ie. to investigate security breach)
- ☐ Direct impairment of ability to perform primary function (erroneous decisions, reduced efficiency, loss of competive edge)
- ☐ Exposure of security weaknesses
- ☐ Other

*Survey used to collect data and determine major consequences for case study.

## CLASSIFICATION CODES

| | | | |
|---|---|---|---|
| Unclassified data | => | Unclassified | => U or 1 |
| Personal data | => | Confidential | => C or 2 |
| Private data | => | Secret | => S or 3 |
| | | Top Secret | => TS or 4 |

## CRITICALITY DEFINITIONS

CRITICAL: Consequences of loss include inaccessibility, loss or unauthorized alteration of such data or applications which could jepordize timely and effective deliverance of primary functions.

Systems that store, process or control assets or resources whose exploitable value exceeds ten million dollars annually.

NON-CRITICAL: All data, applications and hardware not included above.

## SENSITIVITY DEFINITIONS

SENSITIVE: Data classified as "Top Secret", "Secret" or "Confidential".

Personal information and associated records on individuals.

Systems that store process or control assets whose exploitable value falls beween one and ten million dollars annually.

NON-SENSITIVE: All data, applications and hardware not included above.

*Definitions arrived at from discussions with Sergio Guarro Loss of life criteria not applicable in case study.

## DEFINITION GUIDELINES FOR NON-MONETARY SEVERITY CLASSES (NMSC)

0 Damage can be viewed as inconsequential
1 Damage is felt only in local environment and dealt with at that level
2 Damage is directly felt not only in local level, but creates friction but credibility problems with sister organizations and/or central management
3 Damage is felt at the organizational-wide level
4 Damage not only is felt at the organizational-wide level but has organizational security implications
5 Damage has national security implications and potential loss of lives
6 Damage has national security implications and would cause widespread loss of lives

*Classes 5 and 6 were not applicable in the case study system

## MONETARY GUIDELINES FOR THE MONETARY SEVERITY CLASSES (MSC)

0 0 - Materiality Level
1 Materiality Level-50 Thousand
2 50K-100 Thousand
3 100 Thousand- 1Million
4 1 Million-10 Million
5 10 Million-100Million
6 >100 Million

*Materiality Level was defined as $15,000 in the case study

## DEFINITION OF RISK ELEMENTS FOR GENERIC THREATS

Risk Elements (RE) are generated by applying the generic threat-path class matrix to the asset-consequence elements. In abbreviated form we arrive at the following list of risk elements for generic threats:

[T1 P1] [A2] [C1 C2 C7]
[T1 P3] [A2] [ C2 C5 C7]
[T1 P4] [A2] [C1 C2 C5 C7]

[T2 P1] [A2] [C1 C2 ]
[T2 P2] [A2] [C1 C2 C5 ]
[T2 P3] [A2] [C2 ]
[T2 P4] [A2] [C2 C5]
[T2 P5] [A2] [C1 C2] . . . . . .

*Note that during the process of applying threats to assets some consequences can be eleiminated from the risk element notation. This is because, as in the first notation, it is difficult to relate software alteration with the intentional physical attack on a mainframe.

### KEY TO PROPOGATION PATH CLASSES

Human Intentional Threat Types:

| | |
|---|---|
| T1 P1 | Direct Physical Attack |
| T1 P2 | Indirect Physical Attack |
| T1 P3 | Direct Computer- based attack |
| T1 P4 | Indirect Computer-based Attack |

Human Unintentional Threat Types:

| | |
|---|---|
| T2 P1 | Hardware Mishandling |
| T2 P2 | Software Mishandling |
| T2 P3 | Software/Data Errors or Omissions |
| T2 P4 | Procedural Errors or Omissions |
| T2 P5 | Hardware Error/Malfunctioning |

## LPI ESTIMATION USING THE INTEGRATED CONTROL SET VALUE

| ICSV | CER | MPL--> 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0.001 | A | 1 | 1 | 1 | 1 | 2 | 4 |
| 0.01 | B | 1 | 1 | 1 | 2 | 3 | 5 |
| 0.1 | C | 1 | 1 | 2 | 3 | 4 | 6 |
| 0.2 | D | 1 | 1 | 3 | 4 | 5 | 6 |
| 0.5 | E | 1 | 1 | 3 | 4 | 5 | 6 |
| | | LOSS POTENTIAL INDICATOR VALUES | | | | | |

## * MPL SEVERITY CLASS MERGE TABLE

| NMSC | MSC--> 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0(0) | 1(1) | 2(2) | 3(3) | 4(4) | 5(5) | 6(6) |
| 1 | 1(1) | 2(1) | 2(2) | 3(3) | 4(4) | 5(5) | 6(6) |
| 2 | 2(2) | 2(2) | 3(3) | 4(3) | 4(4) | 5(5) | 6(6) |
| 3 | 3(3) | 3(3) | 3(3) | 4(3) | 4(4) | 5(5) | 6(6) |
| 4 | 4(4) | 4(4) | 4(3) | 5(4) | 4(4) | 6(5) | 6(6) |
| 5 | 5(5) | 5(5) | 5(5) | 6(5) | 6(5) | 6(6) | 6(6) |
| 6 | 6(6) | 6(6) | 6(6) | 6(6) | 6(6) | 6(6) | 6(6) |
| | RISK ELEMENT MAXIMUM POTENTIAL LOSS (merged MPL) | | | | | | |

*Conservative values shown without parenthesis used in case study analysis
*Non-conservative values are shown with parenthesis
*Values for MPL in first column are valid only if Materiality Threshold is defined as less than $25,000

Tables reproduced, courtesy of Sergio Guarro

## *SYSTEM ASSETS INVENTORY - Case Study*

| ASSET NUMBER | INFORMATION PROCESSING HARDWARE | | | | | | |
|---|---|---|---|---|---|---|---|
| | ASSET NAME | UNITS | LOSS/U | CLSFCTN | CRITICAL | SNSITIVE | KEEP |
| 1 | Operator Console | 1 | 0.4 | 1 | 0 | 0 | 0 |
| 2 | Mainframes | 3 | 250 | 1 | 1 | 0 | 1 |
| 3 | Mass storage cntrllr | 3 | 18 | 1 | 1 | 0 | 1 |
| 4 | Tape drives | 2 | 25 | 1 | 1 | 0 | 1 |
| 5 | Disk Drives* | 2 | 40 | 1 | 1 | 0 | 1 |
| 6 | Disks | 11 | 10 | 1 | 0 | 0 | 0 |
| 7 | Tape library | 1200 | 0.02 | 1 | 0 | 0 | 0 |
| 8 | Star coupler | 1 | 0.3 | 1 | 0 | 0 | 0 |
| 9 | Ded Microcomputer | 1 | 6 | 1 | 0 | 0 | 0 |
| 10 | Ded Microcomputer | 1 | 118 | 1 | 0 | 0 | 1 |
| 11 | Ded Sun Wrkstations | 2 | 65.5 | 1 | 0 | 0 | 1 |
| 12 | Local terminals | 3 | 2 | 1 | 0 | 0 | 0 |
| 13 | Centralized printer | 1 | 6 | 1 | 0 | 0 | 0 |

| ASSET NUMBER | INFORMATION PROCESSING SOFTWARE | | | | | | |
|---|---|---|---|---|---|---|---|
| | ASSET NAME | UNITS | LOSS/U | CLSFCTN | CRITICAL | SNSITIVE | KEEP |
| 14 | Tutorials | 1 | 0 | 1 | 0 | 0 | 0 |
| 15 | Dbms1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 16 | System diagnostic1 | 1 | 0.2 | 1 | 0 | 0 | 0 |
| 17 | Operating system | 1 | 40 | 1 | 1 | 0 | 1 |
| 18 | Prod 1 application | 1 | 708 | 3 | 1 | 1 | 1 |
| 19 | Assoc prod 1db | 1 | 5 million | 3 | 1 | 1 | 1 |
| 20 | Dec support 1 sw | 1 | 200 | 3 | 1 | 1 | 1 |
| 21 | Assoc Dec support 1 | 1 | 2 million | 3 | 1 | 1 | 1 |
| 22 | Prod 2 application | 1 | 150 | 3 | 1 | 1 | 1 |
| 23 | Assoc prod 2 db | 1 | 1 billion | 3 | 1 | 1 | 1 |
| 24 | ORACLE Rdbms | 1 | 100 | 1 | 1 | 0 | 1 |
| 25 | ORACLE programs | 1 | 20 | 1 | 1 | 0 | 1 |
| 26 | Dec support 2 sw | 1 | 250 | 3 | 1 | 1 | 1 |
| 27 | Assoc Dec support 2 | 1 | 50 | 3 | 1 | 1 | 1 |
| 28 | Dec support 3** | 1 | 20 | | | | |
| 29 | Dec support 4** | 1 | 20 | | | | |

| ASSET NUMBER | NETWORK PROCESSING HARDWARE | | | | | | |
|---|---|---|---|---|---|---|---|
| | ASSET NAME | UNITS | LOSS/U | CLSFCTN | CRITICAL | SNSITIVE | KEEP |
| 30 | Muxes | 1 | 15 | 1 | 1 | 1 | 1 |
| 31 | Terminal servers | 3 | 10 | 1 | 0 | 1 | 1 |
| 32 | Router | 1 | 12 | 1 | 0 | 1 | 1 |
| 33 | Gateway1 | 1 | 25 | 1 | 1 | 1 | 1 |
| 34 | Gateway2** | 1 | 33 | | | | |
| 35 | Value-added ntwrks | 2 | 36 | 1 | 1 | 0 | 1 |
| 36 | Modems | 100 | 0.3 | 1 | 0 | 0 | 0 |
| 37 | Leased lines | 20 | 54 | 1 | 1 | 1 | 1 |
| 38 | Ethernet cable | 1 | 10 | 1 | 1 | 1 | 1 |

| ASSET NUMBER | NETWORK PROCESSING SOFTWARE | | | | | | |
|---|---|---|---|---|---|---|---|
| | ASSET NAME | UNITS | LOSS/U | CLSFCTN | CRITICAL | SNSITIVE | KEEP |
| 39 | SW pckg 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 40 | SW pckg 2 | 1 | 0.1 | 1 | 0 | 0 | 0 |
| 41 | SW pckg 3 | 1 | 2 | 1 | 0 | 0 | 0 |
| 42 | SW pckg 4 | 1 | 0.3 | 1 | 0 | 0 | 0 |
| 43 | SW pckg 5 | 1 | 2 | 1 | 0 | 0 | 0 |

***MATERIALITY THRESHOLD = 15 K***

If an asset is unclassified, is not critical, and not sensitive it is subject to the materiality screen. If direct loss is less than the materiality threshold, it is eliminated (shaded assets).

***CLASSIFICATION KEY:***

Unclassified data .....1
Personal/Confidential data .....2
Private/Secret data .....3
Top secret .....4

***CRITICAL, SENSITIVE & KEEP KEY:***

Yes .....1
No .....0

***OTHER COMMENTS:***

* Denotes that the asset is owned
** Denotes that the asset has been eliminated from the analysis
ALL assets with 1 in the KEEP column remain in the analysis

Case Study Risk Element Defintion

***MATERIAL ASSET-MAJOR CONSEQUENCE MATRIX***

| ASSET NUMBER | MAJOR CONSEQUENCES | | | | | | |
|---|---|---|---|---|---|---|---|
| | C1 | C2 | C3 | C4 | C5 | C6 | C7 |
| A2 | X | X | | | X | | X |
| A3 | X | X | | | X | | |
| A4 | X | X | | | X | | |
| A5 | X | X | | | X | | |
| A10 | X | X | | X | X | X | |
| A11 | X | X | | X | X | X | |
| A17 | X | X | | | X | | |
| A18/19 | X | X | X | X | X | X | X |
| A20/21 | X | X | X | X | X | | |
| A22/23 | X | X | X | X | X | X | X |
| A24/25 | X | X | X | X | X | X | |
| A26/27 | X | X | X | X | X | | |
| A30/31 | X | X | | | X | | X |
| A32/33 | X | X | | X | X | | X |
| A35 | | X | X | X | X | X | |
| A37 | X | X | | | X | | |
| A38 | X | X | X | X | | X | |

*KEY:

C1: Direct hardware or software loss
C2: System interruption and or degradation
C3: Disclosure of information to outside organizations
C4: Disclosure of information to unauthorized individuals
C5: Data and/or software alteration or destruction
C6: Direct impairment of organizational ability to perform the primary mission
C7: Induced diversion of organizational resources

* The criteria for defining the major consequences was developed after discussions with system personnel and management staff. The primary mission was to maintain system operability in order to perform their decision support function.

| Case Study Risk Element Definition | | | | | |
|---|---|---|---|---|---|
| *THREAT PATH / ASSET CONSEQUENCE APPLICABILITY MATRIX* | | | | | |
| | | | | | |
| | THREAT PATH HUMAN INTENTIONAL | | | | |
| ASSET CONSEQUENCE ELEMENT | T1 P1 | T1 P2 | T1 P3 | T1 P4 | |
| | drct phys | indr phys | drct cmpt | indr cmpt | |
| [A2] [C1 C2 C5 C7] | X | | X | X | |
| [A3] [C1 C2 C5] | X | | X | | |
| [A4] [C1 C2 C5] | X | | | | |
| [A5] [C1 C2 C5] | X | | | | |
| [A10] [C1 C2 C3 C4 C5 C6] | X | | X | X | |
| [A11] [C1 C2 C3 C4 C5 C6] | X | | X | X | |
| [A17] [C1 C2 C5] | X | | X | X | |
| [A18/19] [C1 C2 C3 C4 C5 C6 C7] | X | X | X | X | |
| [A20/21] [C1 C2 C3 C4 C5] | X | X | X | X | |
| [A22/23] [C1 C2 C3 C4 C5 C6 C7] | X | X | X | X | |
| [A24/25] [C1 C2 C3 C4 C5 C6] | X | X | X | X | |
| [A26/27] [C1 C2 C3 C4 C5] | X | X | X | X | |
| [A30/31] [C1 C2 C5 C7] | X | | | | |
| [A32/33] [C1 C2 C4 C5 C7] | X | | X | X | |
| [A35] [C2 C3 C4 C5 C6] | X | X | | | |
| [A37] [C1 C2 C5] | X | X | | | |
| [A38] [C1 C2 C3 C4 C5 C6] | X | | X | X | |
| | | | | | |
| | | | | | |
| | THREAT PATH- HUMAN UNINTENTIONA | | | | T2 P5 |
| ASSET CONSEQUENCE ELEMENT | T2 P1 | T2 P2 | T2 P3 | T2 P4 | hw error |
| | hw mshdl | sw mshdl | sw error | proc error | X |
| [A2] [C1 C2 C5 C7] | X | X | X | X | |
| [A3] [C1 C2 C5] | | | X | | X |
| [A4] [C1 C2 C5] | | X | X | X | X |
| [A5] [C1 C2 C5] | X | X | X | X | X |
| [A10] [C1 C2 C3 C4 C5 C6] | X | X | X | | |
| [A11] [C1 C2 C3 C4 C5 C6] | | X | X | | |
| [A17] [C1 C2 C5] | | | X | X | |
| [A18/19] [C1 C2 C3 C4 C5 C6 C7] | | X | X | X | |
| [A20/21] [C1 C2 C3 C4 C5] | | X | X | X | |
| [A22/23] [C1 C2 C3 C4 C5 C6 C7] | | X | X | X | X |
| [A24/25] [C1 C2 C3 C4 C5 C6] | | X | X | | |
| [A26/27] [C1 C2 C3 C4 C5] | | X | X | | X |
| [A30/31] [C1 C2 C5 C7] | X | | | | X |
| [A32/33] [C1 C2 C4 C5 C7] | X | X | X | | X |
| [A35] [C2 C3 C4 C5 C6] | X | X | | | X |
| [A37] [C1 C2 C5] | X | | | | |
| [A38] [C1 C2 C3 C4 C5 C6] | X | | | | |

## *CONTROL REDUCTION FACTOR SENSITIVITY STUDY*

LPI = PCF' X MPL where PCF' = PCF X (1- PCF) X CRF

CRF = REDUCED MPL / CURRENT MPL

* Following the identification of risk elements and the existing controls, assume the presence of one mitigating control (MC1) for RE1 and 3 consequences represented by C1, C2, and C3.

| | | TOTAL MITIGATION | NO MITIGATION |
|---|---|---|---|
| CONSEQUENCES | CURRENT MPL | REDUCED MPL | REDUCED MPL |
| C1 | 100K | 3K | 95K |
| C2 | 20K | 1K | 15K |
| C3 | 50K | 2K | 45K |
| TOTAL | 170K | 6K | 155K |

CRF = .035 (6/170) .91 (155/170)

| PMC# | PCF | 1-PCF | CRF | PCF' | CER | LPI |
|---|---|---|---|---|---|---|
| MC1 | 0.01 | 0.99 | 0.035 | 0.04465 | 0.01 | 1 |
| MC1 | 0.01 | 0.99 | 0.1 | 0.109 | 0.1 | 2 |
| MC1 | 0.01 | 0.99 | 0.2 | 0.208 | 0.2 | 3 |
| MC1 | 0.01 | 0.99 | 0.3 | 0.307 | 0.2 | 3 |
| MC1 | 0.01 | 0.99 | 0.4 | 0.406 | 0.2 | 3 |
| MC1 | 0.01 | 0.99 | 0.5 | 0.505 | 0.5 | 3 |
| MC1 | 0.01 | 0.99 | 0.6 | 0.604 | 0.5 | 3 |
| MC1 | 0.01 | 0.99 | 0.7 | 0.703 | 0.5 | 3 |
| MC1 | 0.01 | 0.99 | 0.8 | 0.802 | 0.5 | 3 |
| MC1 | 0.01 | 0.99 | 0.91 | 0.9109 | 0.5 | 3 |

* MPL (RE1) = 3

*CURRENT CONTROLS - Case Study*

| Preventive: | PCF |
|---|---|
| Security policies are clearly established and understood | 0.5 |
| Security complicance reviews occur on a regular basis | 0.8 |
| Training of personnel in information security procedures adequate | 0.7 |
| Security officers verify whether all staff adhere to security procedures | 0.7 |
| Responsibility for security is clearly assigned | 0.7 |
| | |
| *Guards check identification of individuals entering building | 0.05 |
| *Door to computer room is locked and a card based access control system is used | 0.02 |
| *Badges are worn to indicate authorized persons | 0.05 |
| *Badge holders are reviewed regularly | 0.05 |
| | |
| Physical access is restricted by hardware locks | 0.9 |
| *Visitors are excorted in sensitive areas | 0.02 |
| A challenge procedure is in place whereby strangers are confronted | 0.5 |
| Eating and drinking are not allowed in the computer areas | 0.5 |
| *Personnel policies | 0.2 |
| Employee background checks | 0.4 |
| Constant supervision is given to contract, vendor, service and visiting personnel | 0.52 |
| Employee job training | 0.12 |
| Good morale and work environment | 0.2 |
| Staffed adequately for workload | 0.73 |
| Job assignments are rotated periodically | 0.14 |
| Separation of duties is maintained | 0.73 |
| | |
| *Access control software | 0.01 |
| Privileged accounts are controlled and limited | 0.3 |
| **Common account names such as field, service and default accounts are eliminated | 0.05 |
| **Compliance with password naming (composition) conventions | 0.4 |
| *Forced password change program | 0.02 |
| Automated account manager program for password-based access system | 0.05 |
| *Forgotten passwords given over phone with special infor provided by user | 0.05 |
| Policy for the identification and deletion of temporary and/or old accounts | 0.5 |
| *One user per account policy | 0.1 |
| Automatic logout policy for inactivity at terminal | 0.05 |
| *Time-out periods thwart password guessing attempts | 0.03 |
| Encrypted password file | 0.01 |
| No sharing or posting of passwords | 0.5 |
| | |
| Encryption of sensitive data prevents wiretapping | 0.01 |
| Users not allowed to modify modem hang-up characteristics | 0.3 |
| Fault-tolerant capabilities to cope with component failure and stress conditions | 0.3 |
| Network gives user stable reponse times | 0.1 |
| *Limit the number of people who have knowledge of dial-up line numbers | 0.3 |
| Toll free numbers are changed atleast once a year | 0.9 |
| How to access and use system is documented and available to the user | 0.1 |

| | |
|---|---|
| Required network functionality meets organizational needs | 0.1 |
| Required network performance meets user demands | 0.2 |
| Limit and monitor the usage of network monitoring devices | 0.5 |
| Network gateway and communication interface control | 0.2 |
| | |
| Enforcement of media logging procedures | 0.35 |
| A cart or tray is used to transport media | 0.68 |
| All media is correctly labeled to prevent operator error | 0.03 |
| Damaged tapes and disks are replaced | 0.04 |
| Periodic disk/tape cleaning prevents data loss | 0.25 |
| Loading of software onto system is restricted and controlled | 0.25 |
| Media library physical access is restricted to those with need-to-know | 0.2 |
| | |
| Adequate disposal of obsolete, sensitive or outdated information | 0.27 |
| | |
| Established, scheduled preventive maintenance procedures for hardware | 0.2 |
| Special disk formatting prevents program copying | 0.05 |
| | |
| Structured walkthroughs mandated for programs in development | 0.92 |
| Separation of test and production environments | 0.5 |
| Acceptable sources of software policy | 0.4 |
| Timely, complete updates and version modifications | 0.04 |
| Changes are widely advertised within the user community | 0.26 |
| Program control and security measures embedded in software applications | 0.4 |
| Verification of software integrity after modification process is complete | 0.2 |
| Controls on program libraries and access to production data | 0.4 |
| Only authorized persons can transfer programs to production library | 0.3 |
| Programmers receive only the tools essential to carry out his/her duties | 0.8 |
| Contract "outsiders" are given limited access to information | 0.6 |
| Contract "outsiders" have an obligation to comply with organization's policies | 0.1 |
| Program copies, test data, etc. transfered to authorized person at project completion | 0.96 |
| Naming and labeliing conventions are consistent | 0.4 |
| Suitable testing and quality assurance reviews on all new programs | 0.6 |
| Controls on software tools such as compilers, debuggers, etc. | 0.7 |
| Correct specification of programs (joint-application development) | 0.4 |
| Flexibility of software allows response to changing needs and requirements | 0.2 |
| Functionality of software meets user demands | 0.2 |
| Functionality of network meets organization demands | 0.3 |
| | |
| *Users and jobs cannot use machine unless they have proper clearance | 0.05 |
| *Users select the proper file protections | 0.2 |
| *Subschemas prevent users from viewing data they do not have a need to know | 0.2 |
| Changes are widely advertised within user community before application | 0.9 |
| Classification of information | 0.1 |

*Probability of Control Failure Values are derived from expert opinion
All other Probability of Control Failure Values were developed from the case study system

*CURRENT CONTROLS - Case Study*

| Mitigative: | PCF |
|---|---|
| Prearranged fast delivery of parts and components for replacement and/or repair | 0.2 |
| *Duplicate hardware available for continuation of service | 0.04 |
| Maintenance reports are prepared after every maintenance call | 0.52 |
| System-directed diagnostics | 0.05 |
| Low turn-over of vendor representatives | 0.06 |
| Remote Diagnostic Center available for unresolved system problems | 0.02 |
| | |
| *Logging systems | 0.05 |
| *Last session shown at login time allowing user to notice discrepancies | 0.1 |
| Operator responds effectively to alarm message on console | 0.02 |
| Operations manual correct, current and readily available in crisis | 0.41 |
| Cross training of employees | 0.25 |
| *Operator console log is written to disk | 0.01 |
| Inventories detect loss or theft of media | 0.1 |
| All movement of disks and tape media is logged | 0.33 |
| Strict change control procedures | 0.25 |
| | |
| Major system modifications are followed with update to disaster recovery plan | 0.37 |
| Documented recovery plans | 0.41 |
| Safe storage for all media | 0.03 |
| Backup and recovery plans are tested regularly | 0.4 |
| *Backup data is stored off-site and is recoverable | 0.1 |
| Audit trails and alarms are enabled for specific security risk events | 0.37 |
| Audit trails and monitoring tools are used and logs are reviewed regularly | 0.56 |
| Punitive actions are imposed on security violators | 0.95 |
| Personnel inform management of known security violations | 0.5 |
| | |
| Software performance reports assist in maintenance | 0.05 |
| *Crash followed by automatic checking of programs and data | 0.1 |
| *Read after write on tape and disk drives verifies correctness of write | 0.03 |
| Error and exception reporting | 0.01 |
| Detection of abnormal conditions | 0.01 |
| Self-diagnostics for the detection of software and data errors | 0.01 |
| | |
| *Protocol related error detection codes catch line errors | 0.01 |
| | |
| Team approach used in emergency situations | 0.3 |
| Automatic routing of information around downed links | 0.05 |
| Network processes are relocateable to other nodes | 0.15 |
| *System disconnects users who hang up rather than log off | 0.02 |
| Network fault finding capabilities | 0.9 |
| Accounting facility allows manager to obtain information on network usage | 0.06 |
| Automatic upline dumping of server or system image for problem resolution | 0.01 |
| Trouble-shooting procedures are well-defined and documented | 0.2 |
| Network management monitors and reviews error and event logs regularly | 0.06 |
| Documented procedures for notification and action when security breach is detected | 0.99 |
| The system may be quickly isolated from the network is case of a threat | 0.01 |

| | |
|---|---|
| Periodic internal audits | 0.5 |
| System documentation includes an inventory of network hardware and software | 0.5 |
| Procedures for controls until the system returns to normal are defined and documented | 0.94 |
| Personnel are well trained in backup and recovery procedures | 0.5 |
| Reporting system for acceptance and resolution of network problems | 0.1 |
| Restoration facilities are provided for disconnections | 0.3 |
| | |
| Software is written to be run on any hardware | 0.6 |
| Applications have detailed and well maintained documentation | 0.7 |
| Adequate network documentation (correctness, availability, recovery procedures,etc) | 0.5 |
| Critical files for database are duplicated and stored on a separate device | 0.1 |

*Probability of Control Failure Values (PCF) are derived from expert opinion
All other PCF values were developed for the case study system from data collected.

## RISK ACCEPTABILITY ASSESSMENT RESULTS
(based on the potential loss per single occurrence)

UNACCEPTABLE RISK EVENTS )= $50,000:

Data loss and/or disclosure, degradation or loss of service, delays and inefficiencies due to the bypassing of security provisions to expedite problem solving and/or maintenance.

Disclosure of information to outside individuals due to the lack of supervision for contract, vendor and service personnel.

RISK EVENTS )$10,000 ($50,000:

Unauthorized insertion of new program modules, modifications, or the deletion of existing programs due to inadequate change controls.

Unauthorized hardware alteration by personnel causing the loss or degradation of service, data loss or disclosure.

Physical theft or destruction of production applications due to inadequate media controls.

Incomplete or inaccurate outputs involving production applications causing denial of service to users and potential loss of business to the company.

Software mishandling involving application corruption by unauthorized software usage.

Improperly set file protection attributes caused by software errors or omissions leading to disclosure of information.

Procedural errors, software errors and/or omissions involving both production and decision support applications due to inadequate or non-existent documentation.

## SELECTED BIBLIOGRAPHY

### Books


ABRAMS, 1987 — Abrams, Marshall D., Tutorial: Computer and Network Security, IEEE Computer Society, 1987.

CARROLL, 1977 — Carroll, John M., Computer Security, Security World Publishing Co., Inc, Los Angeles, CA., 1977.

FISHER, 1984 — Fisher, Royal P., Information Systems Security, Prentice-Hall, Inc., Englewood Cliffs, NJ., 1984.

HAMILTON, 1973 — Hamilton, Peter, Computer Security, Auerbach Publishers, Inc., Philadelphia, PA., 1973.

HOFFMAN, 1980 — Hoffman, Lance, Computers and Privacy in the Next Decade, Academic Press, 1980.

HOFFMAN, 1977 — Hoffman, Lance, Modern Methods for Computer Security and Privacy, Prentice-Hall, Inc., Englewood Cliffs, NJ., 1977.

HOFFMAN, 1973 — Hoffman, Lance, Security and Privacy in Computer Systems, Melville Publishing Co., 1973.

HSAIO, 1979 — Hsiao, David K., Kerr, Douglas S. and Madnick, Stuart E., Computer Security, Academic Press, NY., 1979.

JAMES, 1973 — James, Martin, Security, Accuracy and Privacy in Computer Systems, Prentice-Hall, Inc., Englewood Cliffs, NJ., 1973.

NORMAN, 1983 — Norman, Adrian R., Computer Insecurity, Chapman and Hall, NY., 1983.

PARKER, 1973 — Parker, Donn, Computer Abuse, Stanford Reasearch, Inc., 1973.

PARKER, 1976 — Parker, Donn, Crimes by Computer, Scribner, 1976.

PARKER, 1983 — Parker, Donn, Fighting Computer Crime, Scribner, 1983.

RUDIN, 1983 — Rudin, Harry, Protocol Specification, North-Holland and Sole, 1983.

## SELECTED BIBLIOGRAPHY

Journals and Magazines


ABRAMS, 1987 — Abrams, Marshall D., "Network Security: Protocol Reference Model and the Trusted Computer System Evaluation Criteria", IEEE Newtork Magazine, Vol. 1 No. 2 (April1987) pp.24-33.

AMSEL, 1988 — Amsel, Ellen, "Network Security and Access Controls", Computers & Security, Vol.7 No. 1 (Feb. 1988), pp.53-57.

COHEN, 1985 — Cohen, Fred, "A Secure Network Design", Computers & Security, Vol. 4, pp.189-205.

COHEN, 1988 — Cohen, Fred, "On Implications of Computer Viruses and Methods of Defense, Computers & Security, Vol. 7 No. 2 (April 1988), pp.167-184.

CORELIS, 1987 — Corelis, Jon, "Source Code Security: A Checklist for Managers", SIGSAC Review, Vol. 5 No. 2 (Spring 1987), pp.12-16.

CRONHJORT, 1985 — Cronhjort, Bjorn T., "Computer Assisted Reduction of Vulnerability of Data Centers", Computer Security, pp.397-425.

DAVIS, 1987 — Davis, Frank G. and Gantenbein, Rex E., "Recovering from a Computer Virus Attack", The Journal of Systems and Software, Vol. 7 (1987), pp.253-258.

GRANT, 1987 — Grant, Lynn, "DES Key Crunching for Safer Cipher Keys", SIGSAC Review, Vol. 5 No. 3 (Summer 1987), pp.9-16.

GUILLOU, 1987 — Guillou, Louis C. and Ugon, Michel, "Smart Card: A Highly Reliable and Portable Security Device", Advances in Cryptology Crypto 1986, Springer-Verlag, Berlin, Germany, 1987, pp.464-477.

HARPER, 1986 — Harper, Robert M., Jr., "Internal Control in Local Area Networks: An Accountant's Perspective", Computers & Security, pp.28-35.

HIGHLAND, 1985 — Highland, Dr. Harold J., "Microcomputer Security: Data Protection Techniques", Computers & Security, Vol. 4 (1985), pp. 123-134.

JANSEN, 1986 — Jansen, C., "On The Key Storage Requirements for Secure Terminals", Computers & Security, Vol. 5 No. 2 (June 1986), pp. 145-149.

KARGER, 1986 — Karger, Paul A., "Authentication and Discretionary Access Control in Computer Networks", Computers & Security, Vol. 5 (1986), pp. 314-324.

MAKILA, 1985 — Makila, Raimo, "The Relative Measure of Vulnerability - A System in Practice", Computer Security, pp. 225-231.

NEUGENT, 1988 — Neugent, William, "Security Guards: Issues and Approaches", IEEE Communications Magazine, Vol. 26 No. 8 (August 1988), pp. 25-29, 43.

OBERMAN, 1983 — Oberman, M., "Communication Security in Remote Controlled Computer Systems", Advances in Cryptology-Crypto 1986, Springer-Verlag, Berlin, Germany, 1987, pp. 219-226.

O'DONOGHUE, 1987 — O'Donoghue, Joseph, "Strategies Found to Be Effective in the Control of Computer Crime in the Forbes 500 Corporations", SIGSAC Review, Vol. 5 No. 1 (Winter '87) pp. 1-12.

RUTLEDGE, 1986 — Rutledge, Linda S. and Hoffman, Lance J. "A Survey of Issues in Computer Network Security", Computers & Security, Vol. 5, pp. 296-308.

SAARI, 1987 — Saari, Juhani, "Computer Crime - Numbers Lie", Computers & Security, Vol. 6 No. 2 (April 1987) pp. 111-117.

SCHAEFER, 1985 — Schaefer, Marvin, "Security Vulnerabilities in the Automated Office", Computer Security, pp. 427-439.

SCHWEITZER, 1987 — Schweitzer, James A., "How Security Fits In - A Management View", Computers & Security, Vol. 6, pp. 129-132.

SIDHU, 1982 — Sidhu, Deepinder P. and Gasser, Morrie, "Multilevel Secure Local Area Network", Proceedings of 1982 Symposium on Security and Privacy, (April 1982), pp.137-143.

SHAHABUDDIN, 1987 — Shahabuddin, Syed, "Computer Crimes and the Current Legislation", SIGSAC Review Vol. 5 No. 3 (Summer 1983), pp.1-7.

WONG, 1985 — Wong, Ken, "Computer Crime - Risk Management and Computer Security", Computers & Security, Vol. 4 (1985) pp.287-295.

WOOD, 1986 — Wood, Charles C.,"Security Modules: Potent Information Security System Components", Computers & Security, Vol. 5, pp.114-121.

ZAJAC, 1988 — Zajac, Bernard P., Jr., "Dial-up Communication Lines: Can They be Secured?", Computers & Security, Vol. 7 No. 1, (February 1988), pp. 35-36.

## GLOSSARY

| | |
|---|---|
| APPLICATION INTEGRITY | This state exists when the source and object code are in accordance with standards and procedures that have not been altered or destroyed. |
| AUTHENTICATION | The act of verifying the identity of a user or terminal. |
| AUTHORIZATION | The act of permitting the use of system resources. |
| BLOCK CHAINING | Cryptography, linking of multi-block messages by making the encipherment of later blocks dependent on the value of earlier blocks. |
| COMPUTER ABUSE | Any act associated with computers or data communications where victims have suffered or could have suffered a loss and where violators made or could have made gain. |
| CONSEQUENCE | The exposure to potential losses, the effect a threat has on a system asset when controls are defeated or non-existent. |
| CONTROL | Same as countermeasures, safeguards or security measures. It is the capability to exercise direct influence over a given situation or event. |
| CRYPTOGRAPHY | The science of the principles, means and methods for encrypting plaintext and decrypting ciphertext. As a form of access control it can prevent the unauthorized disclosure of sensitive data. |
| DATA CONFIDENTIALITY | This state exists when sensitive data is held in confidence from unauthorized disclosure. |
| DATA INTEGRITY | This state exists when computerized data has not been accidentally or maliciously altered or destroyed. |

| | |
|---|---|
| DEADLOCK | A state of suspended animation which may be caused by a request of conflicting functions. |
| DECRYPTION | Transformation of ciphertext back to its equivalent plaintext by the use of an appropriate key. |
| DISCLOSED DATA | Sensitive or critical data becomes available to certain individuals or the public. |
| ENCRYPTION | Transformation of plaintext into an unintelligible form through the use of key(s). |
| INITIATOR | The originating source of a threat, for example, human-intentional. |
| KEY | Cryptography, a sequence of symbols used to control the operation of encryption and decryption. |
| LEAST PRIVILEGE | To provide the least amount of privilege to a process within the system and to users of the system to accomplish their authorized purpose. |
| MPL | Maximum Potential Loss associated with the single occurrence of one threat event (RE) represented by an equivalent dollar value. |
| NETWORK GATEWAYS | Used to connect dissimilar networks or dissimilar components within a network. |
| PLAINTEXT | Intelligible, usable data before encryption and after decryption. |
| PROTOCOL | A procedure using control information passed between paired layers in order to coordinate processing between those layers. Control information added by one layer is removed and interpreted by the paired layer. |
| RE | Risk Element, a unique descriptive scenario pertaining to a specific threat event. It combines the threat path-asset-consequence descriptors for its identity. |

| | |
|---|---|
| RISK ANALYSIS | A cost effective evaluation of either existing or proposed controls by which risk is minimized in applying security measures commensurate to relative threats, vulnerabilities and the value of resources to be protected. |
| RISK ASSESSMENT | Detailed study of the vulnerabilities threats, potential losses and the effectiveness of security measures; results can be used to develop security requirements and specifications. |
| SEVERITY CLASS | A 6-point scale that represents a range of consequence values. |
| SPOOFING | The deliberate inducement of a user or resource to take an incorrect action as in falsely claiming the identity of a legitimate user. |
| SYSTEM INTEGRITY | The extent to which a system resists penetration. |
| TIME STAMP | Authentication measure indicating the time that the event took place, for example, when a message was sent. |
| THREAT | A hazard, the potential violation of system security. |
| THREAT EVENT | The actualization of a threat. |
| THREAT MONITORING | Provides detection mechanisms for all anticipated penetrations and reporting facilities for monitoring and recording for a secure computer system. |
| TRANSPOSITION | A cryptographic technique in which the characters of a message are rearranged in some manner. |
| TRAP DOOR | A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner such as a random key sequence at a terminal. |

| | |
|---|---|
| TROJAN HORSE | A legitimate software program that contains a section of code that allows the user to perform an unauthorized action such as revealing user's passwords or modifying records in protected files. |
| VIRUS | Malicious software, perhaps a Trojan Horse, which reproduces itself in other systems. |
| VULNERABILITY | A security deficiency, a weakness in the system that makes it possible for a threat to occur. Each vulnerability may be associated with one or more threats. |