NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

SPAN:
A DECISION SUPPORT SYSTEM
FOR SECURITY PLAN ANALYSIS

by

Stephen H. Ramsey

September, 1991

Thesis Advisor: Moshe Zviran

Approved for public release; distribution is unlimited

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED		1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY		3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE		
4. PERFORMING ORGANIZATION REPORT NUMBER(S)		5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b. OFFICE SYMBOL *(If applicable)* AS	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000		7b. ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL *(If applicable)*	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State, and ZIP Code*)		10. SOURCE OF FUNDING NUMBERS

Program Element No.	Project No.	Task No.	Work Unit Accession Number

11. TITLE *(Include Security Classification)*
SPAN: A DECISION SUPPORT SYSTEM FOR SECURITY PLAN ANALYSIS

12. PERSONAL AUTHOR(S) Ramsey, Stephen H.

13a. TYPE OF REPORT Master's Thesis	13b. TIME COVERED From To	14. DATE OF REPORT *(year, month, day)* September, 1991	15. PAGE COUNT 80

16. SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17. COSATI CODES

FIELD	GROUP	SUBGROUP

18. SUBJECT TERMS *(continue on reverse if necessary and identify by block number)*
Decision Support, Computer Security, Security Plan

19. ABSTRACT *(continue on reverse if necessary and identify by block number)*

Computer based information systems provide countless opportunities to improve an organization's functioning and enhance its products or services. They also expose organizations to significant risks as they become increasingly dependent on information resources. To minimize the risks to an organization's information systems, an Information Systems (IS) security plan must be formulated. A Decision Support System (DSS) can provide managers with consistent and consise guidance for the developement and guidance of an IS security plan. SPAN, a Decision Support System for Security Plan Analysis has been developed to provide IS managers with information necessary to make informed IS security plan decisions. This thesis will address how SPAN can be applied for security plan analysis resulting in better and more informed security plan decisions.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS REPORT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a. NAME OF RESPONSIBLE INDIVIDUAL Zviran, Moshe	22b. TELEPHONE *(Include Area code)* 646-2489	22c. OFFICE SYMBOL AS/Zv

83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

Approved for public release: distribution is unlimited.

SPAN: A Decision Support System for Security Plan Analysis

by

Stephen H. Ramsey
Lieutenant, United States Navy
B.S., University of Illinois, 1983

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
September 1991

Author: ____________________________
Stephen. H Ramsey

Approved By: ____________________________
Moshe Zviran, Thesis Advisor

____
William J. Haga, Second Reader

____________________________ for
David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

Computer-based information systems provide countless opportunities to improve an organization's functioning and enhance its products or services. They also expose organizations to significant risks as they become increasingly dependent on information resources. To minimize the risks to an organization's information systems, an Information System (IS) security plan must be formulated. A Decision Support System (DSS) can provide managers with consistent and concise guidance for the development and analysis of an IS security plan. SPAN, a Decision Support System for Security Plan Analysis has been developed to provide IS managers with information necessary to make informed IS security plan decisions. This thesis will address how SPAN can be applied for security plan analysis resulting in better and more informed security plan decisions.

TABLE OF CONTENTS

I. INTRODUCTION

The evolution of the computer industry has provided opportunities for organizations to improve productivity through the use of computer based information systems. As computers begin to fulfill promises made for them, their users become dependent on them. These systems can expose organizations to significant risks as more information flows through them. (Brown, 1971) Thus, an important concern that accompanies the use of information technology is how much security is needed to protect IS resources and how much security actually exists.

An information security professional is responsible for the development, implementation and maintenance of an information security program to protect the integrity, availability and confidentiality of an organization's IS resources. (Jackson, 1990) The focal point of this program is an IS security plan. This plan is a written document that summarizes the resources, identifies the threats and vulnerabilities of the information systems and addresses the IS security needs. (Pfleeger, 1989) SPAN, a decision support system for security plan analysis, supports the IS security planning process and provides a basis for IS security decisions. It assists in IS security planning by formulating a draft IS security plan. Additionally, SPAN allows a security manager to work through "what if" modeling while simulating the effects of various countermeasures.

II. ISSUES IN IS SECURITY PLANNING

The formulation of an IS security plan involves the collection of data concerning IS assets, threats, vulnerabilities and existing countermeasures. An inventory of assets is created, followed by a listing of all of the possible threats to the organization. Existing and proposed countermeasures are evaluated by their effectiveness against the listed threats. (Palmer and Potter, 1989; Pfleeger, 1989; Tomkins, 1991)

A. Identify IS Resources

The first step in security plan formulation is to identify all IS resources in the organization. Resources are collected into the following categories. (Pfleeger, 1989)

1. Data: during execution, stored data, on magnetic media, printed data, archival data, update logs, audit records
2. Documentation: on programs, hardware, system, administrative procedures, the entire system
3. Hardware: central processors, boards, keyboards, monitors, terminals, microcomputers, workstations, tape drives, printers, disk drives, cables, connectors, communications controllers, communications media
4. Personnel: needed to run the computing system or specific programs
5. Software: source programs, object programs, purchased programs, in-house programs, utility programs, operating systems, systems programs, maintenance diagnostic programs

The listing of IS resources has the secondary benefit of creating an inventory of all IS resources in the organization.

B. Assess Threats

Threat analysis is an important element in the development of a security plan. A threat is anything that has the potential to menace, abuse or harm. All possible threats must be itemized for each IS asset. Threats to an organization's IS resources change over time due to changes in employee morale, the workload, the competitive situation, changes in the environment and physical situation. (Browne, 1979)

Security measures can be costly. Therefore, to ensure cost-effective application of security techniques, it is important that a realistic evaluation be made of each potential threat, as well as of the possible countermeasures. (Carroll, 1987)

C. Analyze Vulnerabilities

Based on the threats and probabilities of occurrence, the level of vulnerability of IS resources must be evaluated. A vulnerability is any situation that could cause the loss of secrecy, integrity or availability of an IS resource. (Browne, 1979) The user must assess the impact of an occurrence of any threat on the organization's ability to sustain its mission or execute its primary function.

D. Evaluate Existing Countermeasures

This phase requires the identification of existing countermeasures and evaluating their effectiveness. The effectiveness evaluation is qualitative value subject to the problems of personal preferences or subjectivity. (Zviran, et al, 1990)

E. Evaluate Current Security Level

Based on the results on the preceding steps, the next step calls for the evaluation of the current security level of IS resources and allows for planning of additional countermeasures. (Zviran, et al, 1990) Among the decisions to be made are whether any cost effective countermeasures are warranted, and against which threats the countermeasures should be applied. Determining which countermeasure would be most effective and cost beneficial, can be difficult. An obstacle at this stage is the range of alternative countermeasures. It can become as wide or as narrow as a team's experience or familiarity with them. In addition, these decisions are susceptible to personal preferences or subjectivity. The appropriateness of these countermeasures must be determined based on the operational environment, management philosophy and the organizational culture. (Tomkins, 1991)

F. Formulate a Security Plan

A written IS security plan is the product of this process. It lists all IS assets, their value, relevant threats and vulnerabilities associated with them. The plan includes all countermeasures that are in place and quantifies their effectiveness against specific threats.

Development and implementation of a security plan is not the end of the line. There should be a continuing audit of IS resources to assure the security plan is being properly maintained. (Brown, 1971) Continued p!^nning is required due to the acquisition of new resources and the retirement of existing resources. Computer security is a continuous process.

III. DECISION SUPPORT AND SECURITY PLANNING

A. The Benefits of Decision Support

A decision support system (DSS) is an interactive computer based information system designed to support and enhance managerial decision making in semi-structured and unstructured situations. A DSS should support decision makers in all phases of the decision making process. It allows decisio'. makers to access organizational information, analyze it through some form of model representing an appropriate business or organizational function, and provide a recommended decision. Additionally, a DSS should allow a decision maker to perform sensitivity analysis through "what if" modeling. (Awad, 1988; Bodily, 1985; Sprague and Carlson, 1982; Sprague and Watson, 1989; Turban, 1990)

The decisions involved in establishing an IS security plan are subjective and unstructured. (Zviran, et al, 1990) The crucial elements of risk and vulnerability assessment are subject to personal perceptions of threats to IS resources, the impact of realized threats, and the probability of their occurrence. Although this process calls for a systematic study of all IS assets and corresponding security characteristics, the results might be limited to the knowledge of a specific decision maker. Since different decision makers may place emphasis in different areas, the outcomes may vary from one decision maker to another. A decision support tool can, therefore, provide guidance to reduce the risks associated with inadequate security measures. (Pfleeger, 1989)

B. Existing Packages

Computer-based IS security analysis products fall into two categories; qualitative and quantitative. (Datapro, 1991; Palmer and Potter, 1989; Tomkins, 1991) Qualitative results are usually expressed as loss exposures or annualized loss expectancy (ALE). If the security analysis in to provide an accurate ALE, then the threat frequencies must be established and evaluated. ALE can be defined as the product of the expected loss per harmful event multiplied by the number of times the harmful event is expected to occur in a year's time. Calculations are usually obtained by multiplying the replacement cost of an asset by the annual threat frequency occurrence rate. Since the quantitative method is more exact, it requires more time and effort than the qualitative approach. (Tomkins, 1991)

Qualitative security analysis packages use a scale, either alphabetical, numerical or verbal, assigned to each threat/vulnerability/asset combination. Qualitative security analysis produces values that allow decision makers to see the impact of existing vulnerabilities, the seriousness of a given situation and the potential losses to the organization. (Palmer and Potter, 1989).

The following is a sample of available IS security and risk analysis products. These tools can significantly reduce the amount of human resources necessary for risk analysis, though the ultimate decision concerning security plan formulation remains the responsibility of the owners of the IS resources.

1. The Buddy System Automated Risk Analysis and Management System (Countermeasures, Inc., Hollywood, MD)

The Buddy System is a qualitative methodology that determines the level of vulnerability in 14 areas. End users complete a survey on each system requiring a risk analysis. The software provides a final risk analysis report with conclusions and recommendations. (Datapro, 1990)

2. CAS (Computer Security Consultants, Inc., Ridgefield, CT)

CAS (Computer Aided Security) is an expert system for managing computer security. (Van Zanten, et al, 1987) It consists of a structured approach as well as a broad range of automated tools. The purpose of CAS is to apply the possibilities offered by the computer in achieving and maintaining organizational security.

3. CRAMM (Executive Resource Associates, Inc., Arlington VA)

CRAMM is a menu driven, knowledge-based risk assessment tool and management methodology software support tool. (Datapro, 1990) Menus take the user through three stages of risk assessment and management.

The package performs risk analysis using qualitative means. Once a risk is identified, appropriate countermeasures are recommended. A library of over 1000 countermeasures is included.

CRAMM's standard report contains details of the review including a management summary, valuation of physical, data, and software assets, identified threat and vulnerability details, optimum security requirement details and recommended countermeasures. CRAMM also creates reports that relate directly to operating procedures and physical security.

4. CRITI-CALC (International Security Technology, INC., New York, NY)

CRITI-CALC is a subset of the mainframe based IST/RAMP system. (Datapro, 1990) It is an automated model of a computer security environment used to estimate future annualized loss expectancy to determine the benefit of security measures for any computer environment. It produces over ten reports including Applications

Criticality, Optimum Backup and Recovery Time, ALE Detail and Summary, and Threats Master File.

5. JANBER (Eagan, McAllister Associates, Inc., Lexington Park, MD)

JANBER is a qualitative risk analysis package that can be customized to fit client needs. (Datapro, 1990) It handles up to 18 vulnerabilities and 18 countermeasures and recognizes three data levels.

6. MicroSecure Self Assessment. (Boden Associates, East Willeston, NY)

MicroSecure Self Assessment is a menu driven tool that allows PC users to conduct their own security self assessment. (Datapro, 1990) The software contains an expert system that analyses a customer's data environment.

Three types of reports can be generated: questions/answers by group, tasks, and recommendations. Although the reports are predefined, there is the ability to modify them to meet exact needs if they are printed to a disk file.

7. Risk Watch (Expert System Software Inc., Long Beach California)

Risk Watch supports quantitative and qualitative risk assessments. (Datapro, 1990) Users fill out a parameters screen, customize threat data, enter asset information, and answer questions. Risk Watch matches the user's data against its expert system and identifies weaknesses in the security plan, what safeguards should be implemented, and how much each safeguard will save the organization.

8. RiskPAC (Computer Security Consultants, Inc., Ridgefield, CT)

RiskPAC is an interactive, PC-based, automated, qualitative/quantitative risk assessment software product with an expert system engine. (Datapro, 1990; Kelly, 1988) It is used to run questionnaires that embody a knowledge base of data security. The survey process consists of up to three levels, such as DP environment, processor(s), and applications. Questions covering 26 risk categories are asked in each level, producing a ranked listing of processors and applications with risk levels and vulnerabilities.

9. SBA's BASIC Software Procedures (Small Business Administration)

The Small Business Administration has developed an automated system that provides decision support tools for its managers to define systems security needs and responsibility. (Powell, 1988) The software collects and organizes security plan data required by the Computer Security Act of 1987. The program takes managers through the process of identifying sensitive systems according to name, type, the level of aggregation, the hardware/software environment, operational and technical controls and the federal security regulations that must be met. The SBA also uses a program development guide that defines the needs and responsibilities regarding system security. The guide also includes a formula for risk management. Risks are measured through a systematic evaluation that quantifies the impact of losses and the probability of losses occurring.

IV. SPAN DEVELOPMENT

A. Requirements

SPAN is a complex decision support tool designed to assist IS security managers in the development of an IS security plan. As such, it had to be designed with the following characteristics in mind. (Turban, 1990)

1. It must have the ability to support the solution of a complex problem.
2. It must be able to respond quickly to unexpected situations that result in changed conditions.
3. It must allow the user to try several different strategies under different configurations via "what if" analysis.
4. It must provide improved management performance and effectiveness.
5. It must derive consistent and objective decisions.

To satisfy the demands of an IS security analysis tool, SPAN had to consolidate a wide array of threat and countermeasure information that comprise a highly complex relational database. The system required strong error trapping and data integrity capabilities. It also required user friendly data entry screens with highly structured entry and edit procedures. Finally, it was imperative that the system produce reports that present information in a user definable manner.

SPAN was intended to be a micro-computer based application. This required SPAN to run successfully on any of the IBM family of personal computers or a 100% IBM-compatible personal computer.

B. Software Selection

Two development tools and methodologies were considered. Both were centered on Borland International's Paradox®. The first alternative was to create SPAN's dialogue subsystem and model base using the C++ programming language. The data module would consist of tables created by Paradox and integrated into the system the Paradox Engine. The Paradox Engine provides an Application Programming Interface that allows the manipulation of Paradox tables. The benefit of this approach was the speed and size of the resulting application. The major drawback was the requirement to manually design and code all of the programs forms, reports and data integrity features.

The methodology chosen was to use Paradox and PAL™ (Paradox Application Language™) for the entire development of SPAN. Paradox is the most highly rated PC-based relational database management system on the market. (Kalman and Poor, 1991) Paradox easily met the requirements set forth above.

Paradox is a full-featured relational database management program that can be used either as a stand-alone system on a single computer or as a multiuser system on a network. SPAN was created with the most recent release of Paradox, version 3.51.

Paradox includes two development tools, Paradox Personal Programmer™ and PAL. Personal Programmer is an application generator that enables a user to develop custom single-user database applications without programming. Personal Programmer is best used to generate prototypes of applications because it is limited in its abilities and creates code that is very difficult to modify.

PAL is a full featured structured programming language that is completely integrated with Paradox. Paradox provides many objects that are necessary in a database application. Objects include tables, forms, reports and queries. Other Paradox features are also available, such as record sorting, crosstabs, complete multiuser capabilities and presentation quality graphs. With PAL, all these objects and features are at the programmers disposal. PAL programs are shorter and more powerful than other database management computer applications because they have unlimited access to all of Paradox's objects.

Two PAL programming tools were used to enhance SPAN. The inspiration for some of SPAN's help routines was taken from DESKTOP for Paradox by Kallista, Inc. (© 1988, 1990 Kallista, Inc.) DESKTOP is a collection of PAL routines written to make working in the interactive Paradox environment easier and more enjoyable. It provides a useful set of functions for developers of Paradox applications.

A valuable source of PAL functions and examples used in SPAN was *PAL by Example* (Zenreich and Kocis, 1991). The accompanying WaitPlus Pro (©1990-1991 PAL by Example) was used to create many of SPAN's data entry and edit routines. WaitPlus Pro is a series of PAL procedures that standardize user access to data.

SPAN was designed to run as a stand alone application. Although SPAN was developed with Paradox, it does not require Paradox to run. Instead, SPAN is distributed with Paradox Runtime, which provides almost all of the functions included in Paradox itself. It allows SPAN to exploit the full range of Paradox's features. However, Paradox Runtime does not perform certain tasks that Paradox itself does, because Runtime is simply a tool to run Paradox applications.

V. SPAN OVERVIEW

A. System Requirements

SPAN was designed to work on any of the IBM family of personal computers or a 100% IBM-compatible personal computer. The program requires a hard disk with a minimum of four megabytes of free space, and a high density 5¼" disk drive. SPAN needs 512K or more of internal memory, but performance will improve drastically if extended or expanded memory is available. A color monitor is highly recommended.

B. Design Overview

As in most decision support systems, the three components of SPAN include a dialogue subsystem that serves as the interface between a user and the system, a knowledge base module, and a model base. (Sprague and Carlson, 1982; Sprague and Watson, 1989; Turban, 1990)

1. Dialogue

SPAN's dialogue subsystem consists of a menu-driven user interface with a built-in context sensitive help system. The menus and screen formats guide a user through the functional operations of the various activities involved in IS security planning.

2. Data

SPAN's database subsystem is based on a relational data model. Data files of threats and countermeasures are predefined and consist of data about common threats to each resource type, specific countermeasures and countermeasure effectiveness against specific threats. Data for this element was gathered from a wide variety of sources.

(Alexander, 1991; Bequai, 1983; Bidgoli and Azarmsa, 1989; Browne, 1979; Carroll, 1987; Diehl, et al, 1991; Hsiao, et al, 1979; Jackson, 1990; Palmer and Potter, 1989; Ruthberg and McKenzie, 1977; Lane, 1985; Walker and Walker, 1977)

User defined resource files are used to store information about locations and IS resources in a particular organization. Data contained in these files include location, resource type, resource description and level of criticality to the organization. Other available data include model number, serial number, dollar value and acquisition date. By means of the dialogue subsystem, a user can update these files by using the insert, edit and delete functions. The user also may view the contents of these files and produce reports.

3. Model

SPAN's model base consists of processes that are employed to support decision making. These are used to evaluate countermeasures against various levels of vulnerability and recommend an appropriate mix of countermeasures to an organization. The models were developed using algorhythms written in PAL and queries created with Paradox's Query by Example feature.

C. Sequence of Operations

SPAN's basic operational flow is comprised of seven activities. These activities are normally conducted in consecutive order.

1. Identify All Locations Containing IS Resources

All locations (offices, computer centers, storage facilities, etc.) containing one or more IS resource are entered into the system, indicating the location identification, description, and level of criticality assigned to this location.

2. Identify All IS Resources

An itemized list of all IS resources in each location is entered in SPAN's database. The data entered for each IS resource includes resource type (data, documentation, hardware, personnel, software), name, description, model number, serial number, value, acquisition date and criticality. The default value for the resource's level of criticality equals the one assigned its location.

3. Identify Relevant Threats

SPAN's database contains a table of common threats for each type of IS resource. This table helps a user in evaluating the threats to a particular organization. Threat assessment is performed separately for each location and IS resource. The system presents the user with a list of all location and IS resources. The user is required to select those threats that might apply to a specific location or IS asset. In addition to the pre-defined set of common threats, a user can add other threats that do not appear in SPAN's database.

4. Evaluate Probability of Occurrence

After threat identification is completed, the user provides the system with probabilities of occurrence. Probability of occurrence refers to the likelihood that a specific threat will occur. Knowing the probability of occurrence of a threat is a major factor in evaluating the countermeasure that will be most effective against it. (Ruthberg and McKenzie, 1977) This estimate is measured on a ten point scale (one, unlikely to occur; ten, likely to occur).

5. Assess Vulnerability

Vulnerability assessment represents the impact of any particular threat on the organization. During this stage each location and resource is presented along with all of its associated threats. The user is asked to assess the impact of an occurrence of any of these threats on the organization's ability to function. A ten point scale is used (one, no impact on organizations ability to function; ten, organization cannot function).

6. Select Existing Countermeasures

The next step in the security planning process identifies and assesses existing countermeasures. The user must select those countermeasures that are implemented for each location and resource.

7. Formulate a Draft Security Plan

The last stage is the formulation of a draft security plan. SPAN evaluates the existing countermeasures in view of the threats, their probability of occurrence and the risks they impose on the organization. It then recommends new security measures. The system evaluates all potential countermeasures against the threats identified during the threat and vulnerability evaluation phases. It proposes a mix of recommended countermeasures and lists them according to their effectiveness. This information is reported in a written draft that systematically documents all inputs (locations, resources, threats, probabilities, vulnerabilities and existing countermeasures) and suggests additional countermeasures to improve IS security. Based on this preliminary draft, a user can perform sensitivity analysis via the sensitivity module and examine the impact of changes in threats, probabilities and countermeasures on the security plan.

D. Control Mechanisms

Each SPAN session begins at the main menu. (Figure 1) It is the highest level in the menu hierarchy and it reflects SPAN's structure.

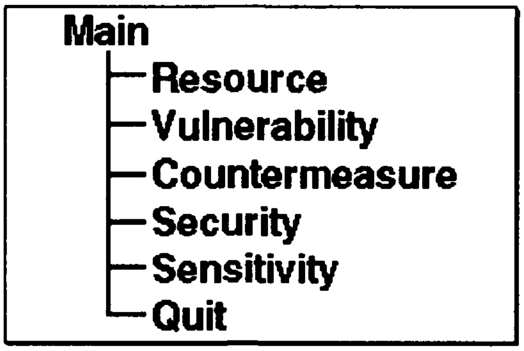


Figure 1 Main Menu Structure

The resource management option provides the capability to build and manage the resource database by adding new IS resources, modifying or deleting existing resource data, viewing data and producing reports. (Figure 2) The resource database contains information about individual resources and all locations in the organization that contain IS resources. Reports are available by location, resource type, value, or a resource summary report for the entire organization.

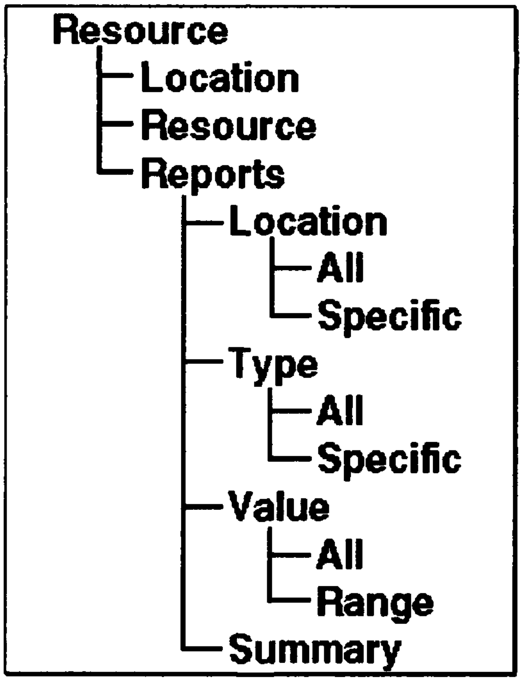


Figure 2 Resource Menu Structure

The vulnerability assessment option provides the user with five main functions. (Figure 3)

1. Update the system's list of possible threats by adding, modifying or deleting potential threats.

2. Identify and select those threats that apply to the entire organization, a specific location, a certain type of IS resource or to a particular resource.

3. Assign a perceived vulnerability level to any resource according to the specific threats to it. Vulnerabilities are assigned on a ten point scale (one, extremely low vulnerability; ten, extremely high vulnerability).

4. Revise an update threat and risk data associated with the entire organization, a specific location, a certain type of IS resource, or a particular resource.

5. Produce reports to represent which locations, resource types or specific resources are most vulnerable to threats. This vulnerability representation aims to define where the greatest exposures, by threat or valuation, exist.

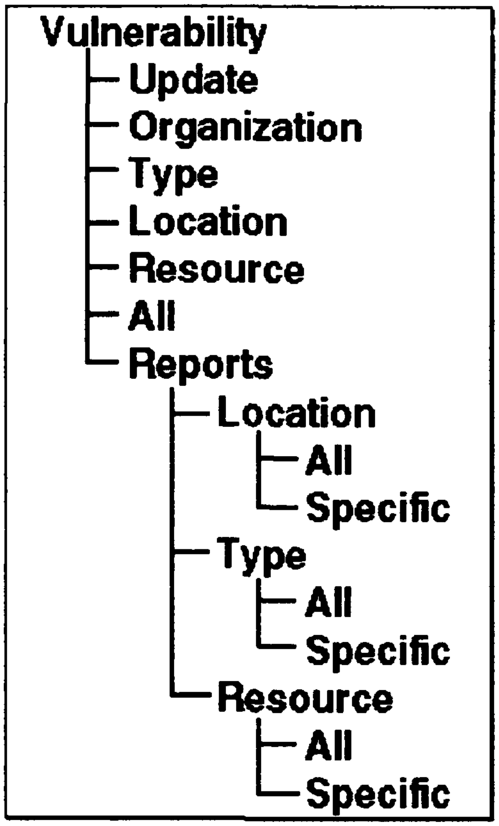


Figure 3 Vulnerability Menu Structure

The countermeasure management option allows a user to identify a profile of existing countermeasures. (Figure 4) The user may update the system's list of countermeasures by adding, modifying or deleting available countermeasures. Reports can be generated by location, resource criticality, threat or specific countermeasure.

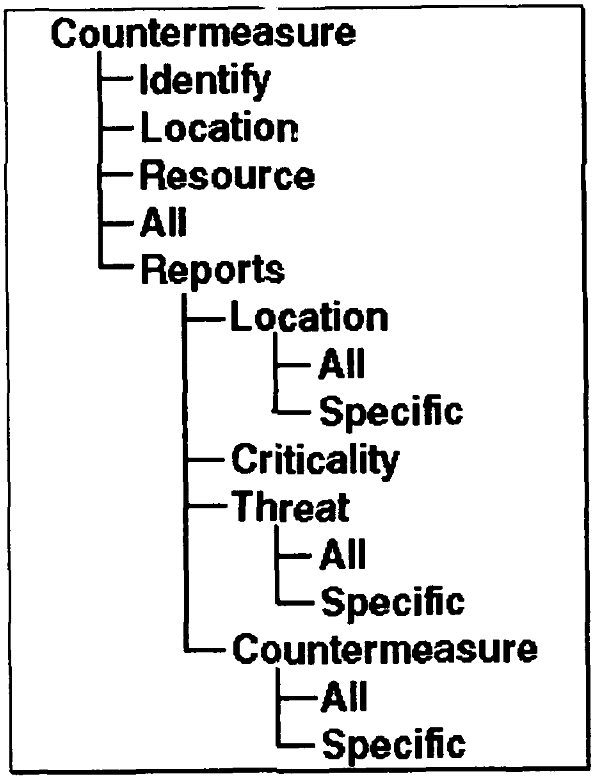


Figure 4 Countermeasure Menu Structure

The security analysis function correlates each vulnerable exposure to protection affected by existing countermeasures. (Figure 5) An effectiveness score on a ten point scale (one, ineffective; ten, highly effective) is incorporated into SPAN and allows the user to assess an effectiveness level of existing countermeasures. This allows the user to perform the following operations.

1. Identify locations, specific resource types or particular resources with potentially inadequate countermeasures in place.

2. Rank locations and resources warranting further study of countermeasure funding.

3. Approximate the effectiveness of the proposed countermeasures.

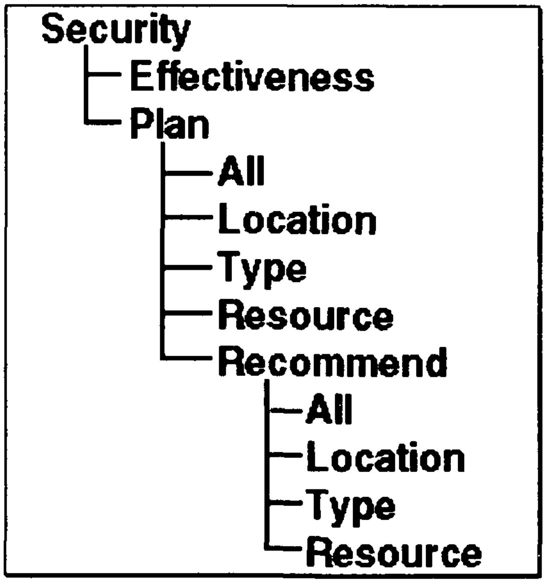


Figure 5 Security Menu Structure

Another function included in this menu is security plan formulation. This provides the user with the ability to produce a draft IS security plan as the product of the security analysis process.

The sensitivity analysis option allows the user to perform further analysis through "what if" scenarios. (Figure 6) These scenarios are created by entering additional data elements or parameters to the existing database and examining their impact on the system's outputs. The changes performed during these scenarios are saved in a temporary file and do not alter SPAN's database.

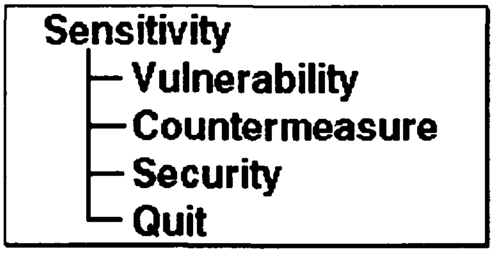


Figure 6 Sensitivity Menu Structure

E. Strengths and Weaknesses

SPAN will prove to be a highly useful tool to any IS manager. The system will assist in the generation of an IS security plan, as well as create and maintain a database of IS resources. SPAN is a reliable product and has undergone extensive testing.

Paradox's objects, one of its strengths, unfortunately provide one of SPAN's minor weaknesses. SPAN requires at least four megabytes of free disk space. Each object consists of one or more separate files. As the number of forms and reports increase, so does the requirement for free disk space. This factor also contributes to the relatively slow speed at which SPAN moves from one operation to another.

F. Future Development

Although SPAN is a versatile tool, there is room for further expansion. With this in mind, SPAN was built with a highly structured design.

SPAN is currently configured to be used by a single organization. SPAN's first enhancement will probably give it the ability to manage the resources and security planning for multiple organizations. System's analysts and security consultant's would then need only one copy of SPAN to handle all of their clients' data.

SPAN was designed as a stand-alone system. If future SPAN enhancements promote the need for a distributed application, SPAN can be easily modified. Qualitative aspects also may be added to future versions of SPAN.

VII. CONCLUSIONS

As organizations become more dependent on smooth functioning IS resources, an increasing number of them are prepared to implement adequate security measures to protect these resources. A prerequisite to implementing an effective set of countermeasures is the formulation of an IS security plan.

The security analysis process can be laborious due to the time and resources required for data collection and analysis. While there are few shortcuts to data collection, the use of SPAN to evaluate the suitability of countermeasures can significantly reduce the effort required. Also, the capability to do "what if" modeling to determine the potential results caused by changes in threats and countermeasures can be quite beneficial.

SPAN is a tool, not a solution, for security plan analysis. It provides the framework for analysis, but the tasks of gathering asset information, analyzing results and implementing recommendations still lie with the IS security manager.

APPENDIX A

SPAN USERS MANUAL

A. About SPAN

SPAN is a DSS developed to help IS security managers carry out key activities of IS security planning and resource management. SPAN allows managers to create a draft security plan based on threats to the organization and its resources. The system also provides a list of suggested countermeasures, based on the applicable threats. SPAN provides IS managers with detailed reports based on user selected parameters. It is a user friendly system that will prove to be an invaluable tool to any organization with IS resources.

The SPAN manual uses special typefaces to help distinguish between menu commands, form names, field names, keys to be pressed and text that is typed. These are printing conventions only and do not apply to section headings. Table A-1 lists these conventions.

PRINTING CONVENTIONS

Convention	Elements
Bold	Menu Title
Initial Letter Bold	Menu Commands
Bold Italics	Forms and Reports
Italics	Fields
Alternate Bold Font	Keypress
SMALL CAPS	User Entered Information

Table A-1

1. Installing SPAN

a. System Requirements

SPAN is designed to work on any of the IBM family of personal computers or a 100% IBM-compatible personal computer. The program requires a hard disk with a minimum of four megabytes of free space, and a high density 5¼" disk drive. SPAN needs 512K or more of internal memory, but performance will improve drastically if extended or expanded memory is available. SPAN may be run under Microsoft® Windows™, though it is recommended that the installation procedures be executed from the DOS system prompt.

b. Installing Files

SPAN must be installed and run from a hard disk, You must first determine the directory in which to install SPAN. If the directory does not already exist, it must be created. To create a new directory, use the DOS **MD (MKDIR)** command. The following command will create a directory named SPAN:

```
MD SPAN
```

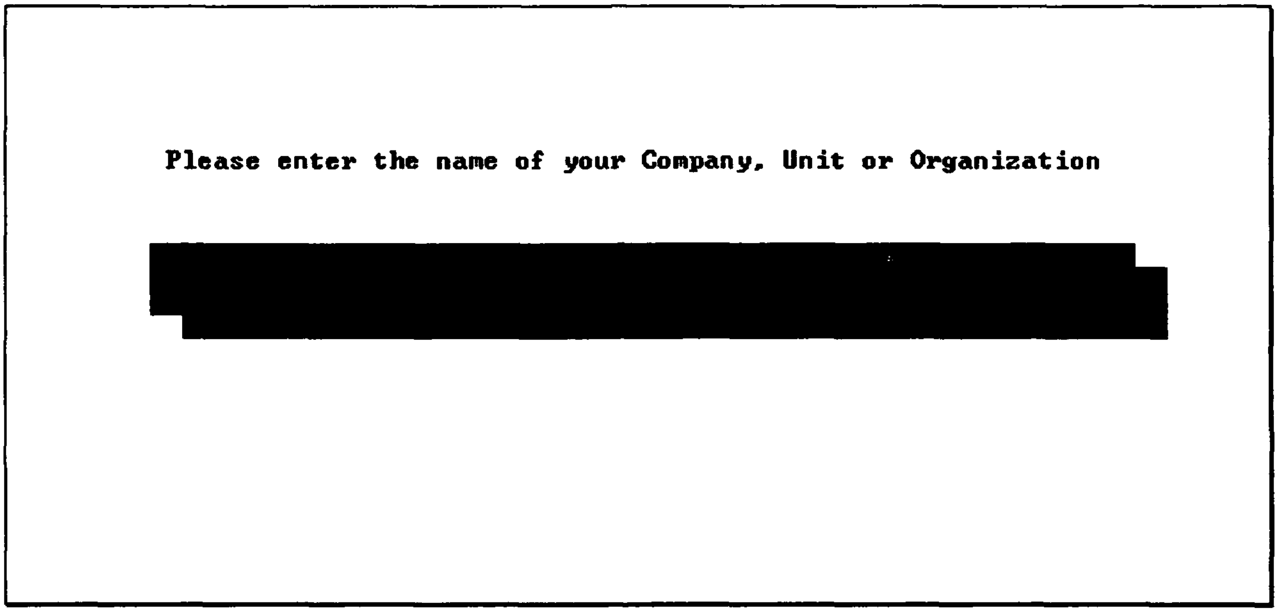
The directory will be created as a subdirectory of the current directory.

SPAN's files must now be copied to the newly created directory. Insert the SPAN disk in a high density 5¼" disk drive and copy all files. This can be accomplished by using the DOS **COPY** command. The following command will copy all files from the disk in drive a: to the current directory.

```
COPY A: *.*
```

At this point, all of SPAN's files are in the SPAN directory, but they are in an unusable compressed format.

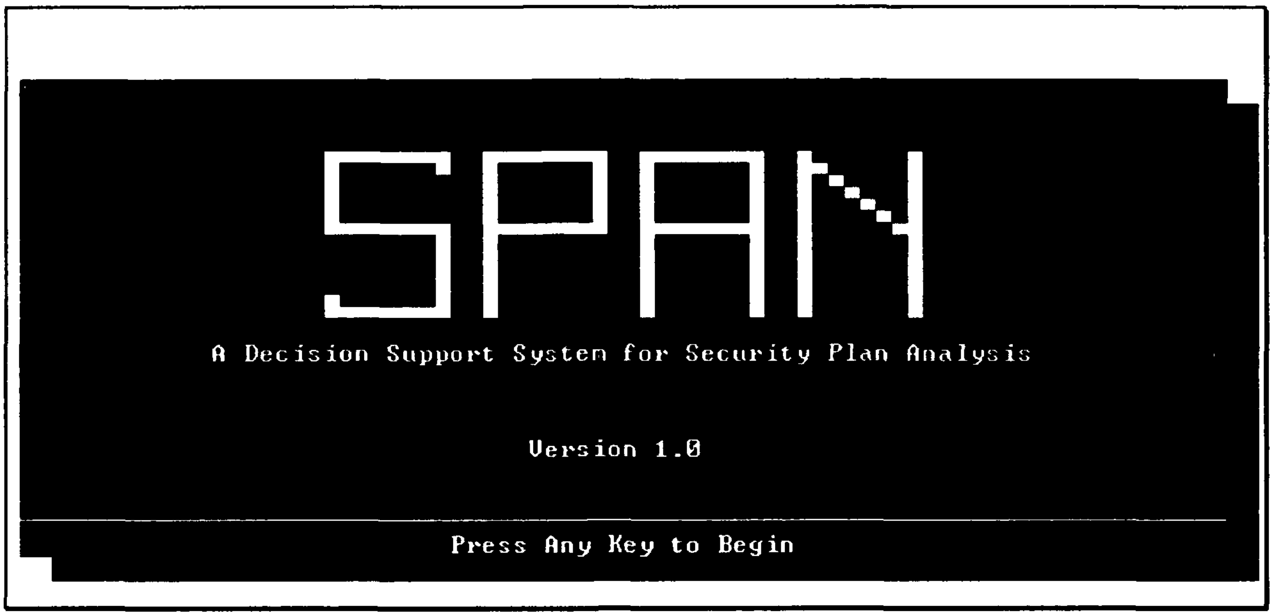
The file decompression and setup process begins with the **INSTALL** command. You must be certain that SPAN's files are in the desired subdirectory and that there is enough free space available. Once SPAN's install procedure begins, it cannot be stopped. Your first SPAN session will begin immediately following the decompression process. You will next be presented with a screen asking you to enter the name of your company, unit or organization. (Figure A-1) Carefully type the name and press **Enter**. This information is required and becomes a permanent part of SPAN's database. This screen only appears at the beginning of the first SPAN session.



```
Please enter the name of your Company, Unit or Organization
```

Figure A-1 Name Entry Screen

After the successful completion of the installation procedure, you will be presented with SPAN's opening screen. (Figure A-2) Press any key to exit the opening screen and begin your first SPAN session.



SPAN

A Decision Support System for Security Plan Analysis

Version 1.0

Press Any Key to Begin

Figure A-2 Opening Screen

2. Starting SPAN

SPAN is started automatically at the completion of the installation process. Further SPAN sessions are started by typing **SPAN** at the DOS prompt. Make sure the DOS system prompt for your hard disk (usually drive C) is on the screen. Type **CD\SPAN** to change the current directory to \SPAN. Type **SPAN** and press **Enter** to begin your session. If SPAN is used under Microsoft Windows, use the **WINSPAN** command to start SPAN.

3. The Menu System

SPAN's menus appear across the top of the screen. They are organized on different levels in a top-down, hierarchical way, so that one menu leads to another submenu. You can narrow the range of available choices until you have arrived at the selection you wish to make.

At the top of this menu structure is SPAN's **Main** menu, which appears immediately following SPAN's opening screen. (Figure A-3) All of SPAN's menus are similar in structure to the **Main** menu. Menu choices are selected by using the **right-** or

left-arrow keys to highlight a menu choice and then pressing **Enter**. **Home** moves the cursor to the first menu choice. **End** goes to the last menu choice. You also may press the key of the first letter of the desired menu choice. If two or more menu choices begin with the same first letter, SPAN's menu will collapse to show the remaining possible selections. You can then select the desired menu choice with the arrow keys, or continue typing the letters in the desired menu choice until all the other possible choices have been eliminated.

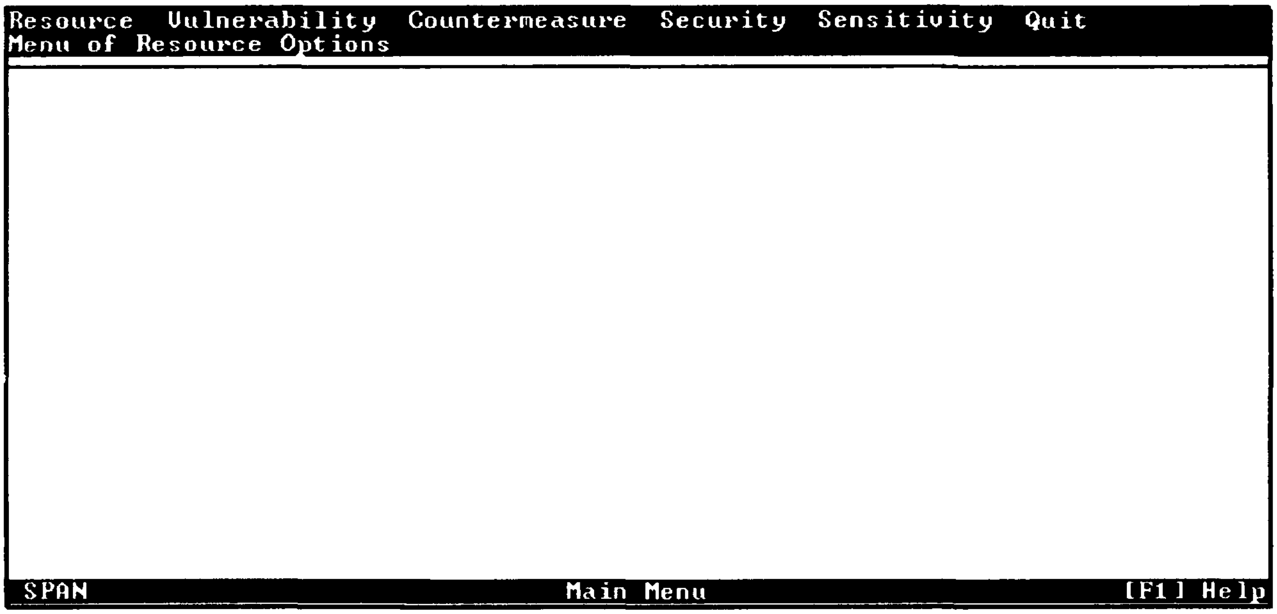
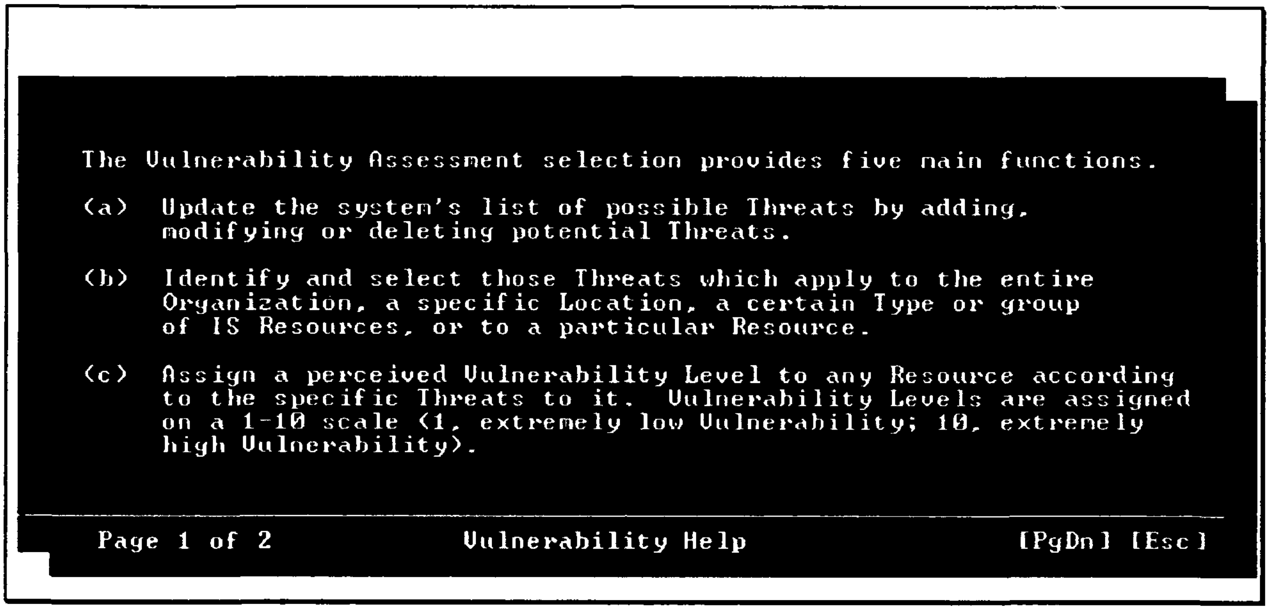

Resource Vulnerability Countermeasure Security Sensitivity Quit
Menu of Resource Options
SPAN
Main Menu
[F1] Help

Figure A-3 Main Menu

As you move the cursor through the menu choices, you will notice that a description of each selection is displayed on the second line of the screen. At the bottom of screen appears an information bar that includes the name of the current menu and other helpful information.

4. Getting Help

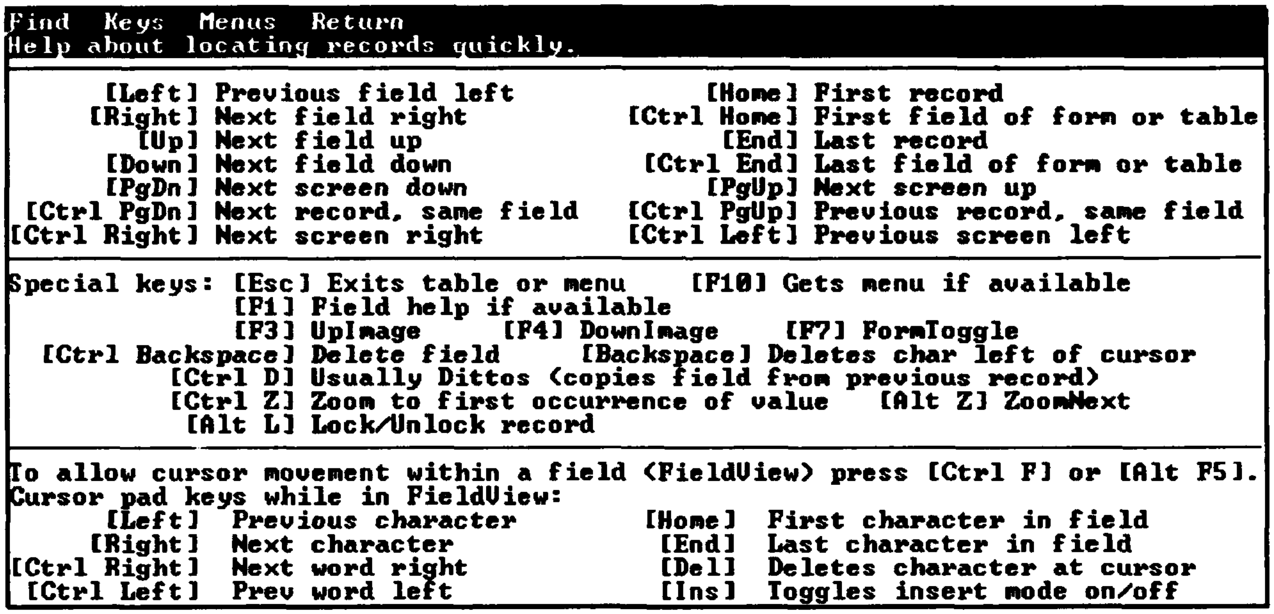
SPAN provides context sensitive help screens for every menu choice. To get help from any SPAN menu, press **F1**. A help screen will appear giving information on the current selection. (Figure A-4) The information bar on the bottom of the help screen will alert you to the number of help pages available. You can navigate between pages by using the **Page-Up** and **Page-Down** keys. Help is exited by pressing the **Esc** key.



```
The Vulnerability Assessment selection provides five main functions.

(a)  Update the system's list of possible Threats by adding,
     modifying or deleting potential Threats.

(b)  Identify and select those Threats which apply to the entire
     Organization, a specific Location, a certain Type or group
     of IS Resources, or to a particular Resource.

(c)  Assign a perceived Vulnerability Level to any Resource according
     to the specific Threats to it.  Vulnerability Levels are assigned
     on a 1-10 scale (1, extremely low Vulnerability; 10, extremely
     high Vulnerability).

  Page 1 of 2              Vulnerability Help              [PgDn] [Esc]
```

Figure A-4 Menu Help

Help is also available from SPAN's data entry forms. Pressing **F1** will display field specific help. SPAN's field specific help is in the form of lookup tables that exhibit all valid entries for the current field. This feature is helpful for entering information on many of SPAN's forms. Once the lookup table has been called, you may use the cursor keys to scroll through the table to find the record with the value for which you are looking. You may press **F2** when you have found the record with the value in which you are interested. This fills in the current value in the first field of the lookup table into the current field of the form. Press **Esc** to return to the form you are editing without entering a value. The **F10** key will display general help about entering data and navigating through the form. (Figure A-5)



```
Find  Keys  Menus  Return
Help about locating records quickly.

      [Left] Previous field left            [Home] First record
     [Right] Next field right          [Ctrl Home] First field of form or table
        [Up] Next field up                   [End] Last record
      [Down] Next field down            [Ctrl End] Last field of form or table
      [PgDn] Next screen down               [PgUp] Next screen up
 [Ctrl PgDn] Next record, same field   [Ctrl PgUp] Previous record, same field
[Ctrl Right] Next screen right         [Ctrl Left] Previous screen left

Special keys: [Esc] Exits table or menu    [F10] Gets menu if available
              [F1] Field help if available
              [F3] UpImage      [F4] DownImage     [F7] FormToggle
  [Ctrl Backspace] Delete field     [Backspace] Deletes char left of cursor
        [Ctrl D] Usually Dittos (copies field from previous record)
        [Ctrl Z] Zoom to first occurrence of value   [Alt Z] ZoomNext
         [Alt L] Lock/Unlock record

To allow cursor movement within a field (FieldView) press [Ctrl F] or [Alt F5].
Cursor pad keys while in FieldView:
      [Left]  Previous character        [Home]  First character in field
     [Right]  Next character             [End]  Last character in field
[Ctrl Right]  Next word right            [Del]  Deletes character at cursor
 [Ctrl Left]  Prev word left             [Ins]  Toggles insert mode on/off
```

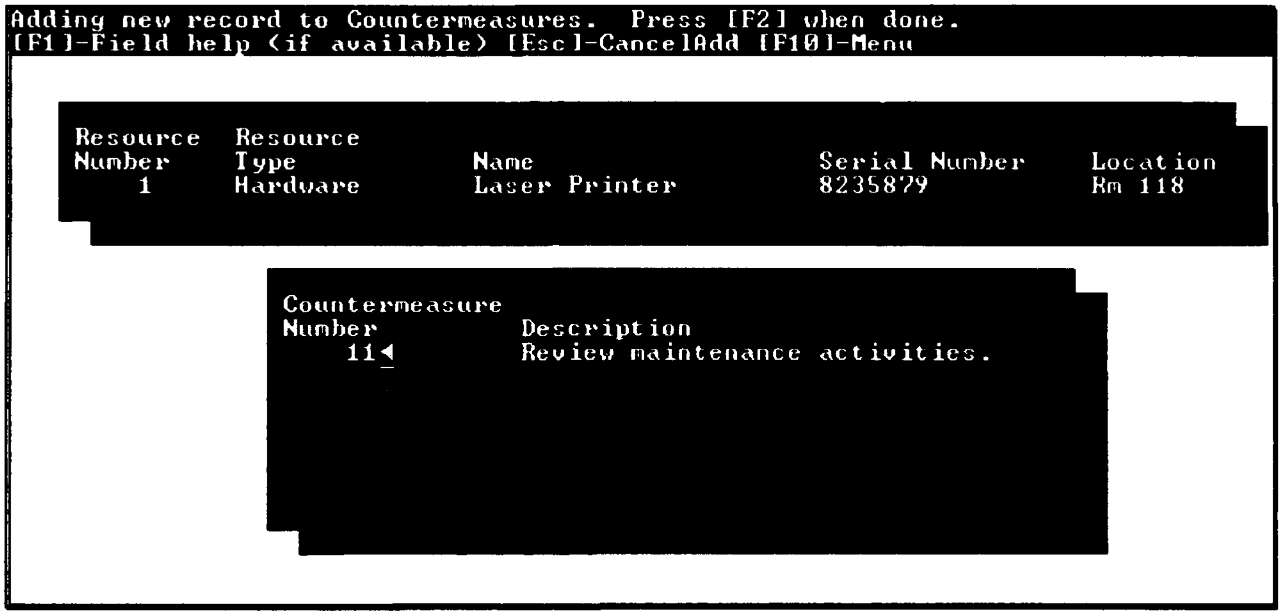
Figure A-5 Form Help

5. Entering and Changing Information

The data entry interface is consistent throughout SPAN. Each form uses the same set of commands for inserting, deleting and editing records.

SPAN's forms provide an information bar at the top of the screen that lists some of the available commands. These commands will vary depending upon the position of the cursor and the selected function. For example, occasionally you may not insert or delete records. In this case, the information bar will not list the commands for insert or delete.

Some of SPAN's forms contain two separate boxes, or images. (Figure A-6) Pressing **F4** moves the cursor from the upper image to the lower image. **F3** moves the cursor from the lower to the upper image. As you move from one image to another, the information bar will change, depending on the operations allowed in each image.



```
Adding new record to Countermeasures.  Press [F2] when done.
[F1]-Field help (if available) [Esc]-CancelAdd [F10]-Menu

  Resource   Resource
  Number     Type            Name                     Serial Number     Location
     1       Hardware        Laser Printer            8235879           Rm 118

        Countermeasure
        Number          Description
            11          Review maintenance activities.
```

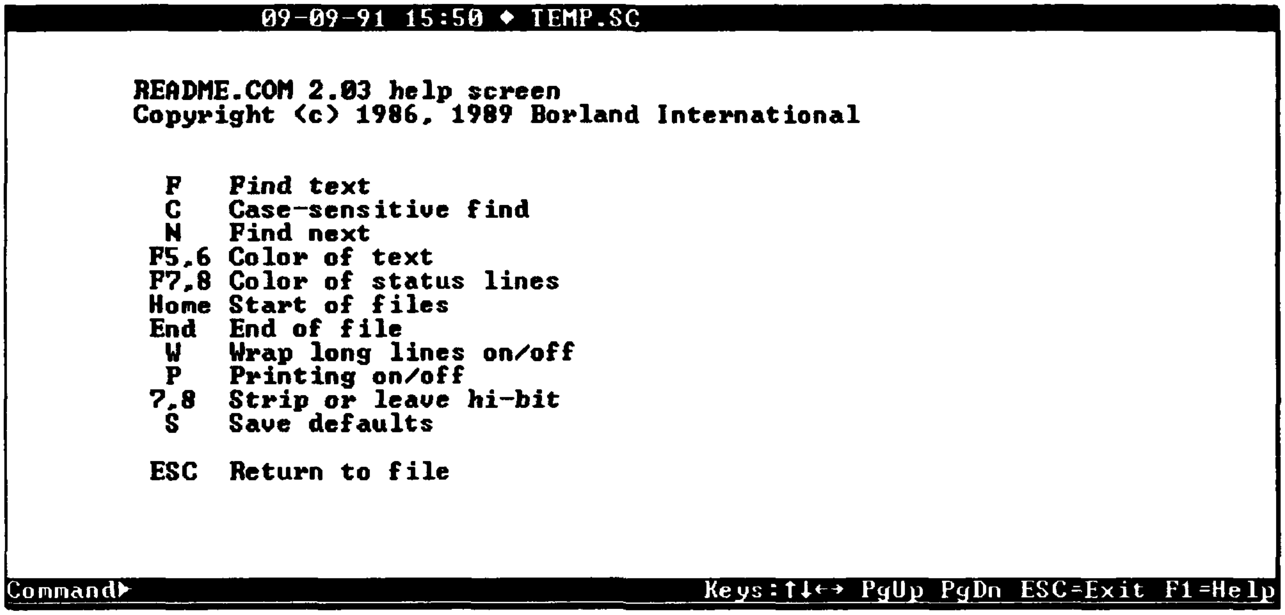
Figure A-6 Sample Form

The numeric keypad can be used to move the cursor around on a form and to display other records on the form. If a field on a form cannot be modified, the cursor will not land on that field. If the cursor is on the last field of a form, either the **right-** or **down-arrow** moves to the first field of the next record. Similarly, the **left-** or **up-arrow** can be used to move to the previous field of the form, or from the first field to the last field of the previous record. **Page-Down** displays the next record on the form, and **Page-Up** displays the previous record. Help is available by pressing **F10.**

6. Reports

One of SPAN's most useful features is its ability to generate custom reports. SPAN provides 49 different reports in which the user can may specify the contents, format and range of output. Reports can be sent to the printer or screen.

Screen reports can be viewed and browsed in a variety of ways. You may locate text, change the default colors, and even print the report. Pressing **F1** while the report is on the screen will bring up a list of available commands (Figure A-7).



```
                  09-09-91 15:50 ♦ TEMP.SC

      README.COM 2.03 help screen
      Copyright (c) 1986, 1989 Borland International

       F   Find text
       C   Case-sensitive find
       N   Find next
       F5,6 Color of text
       F7,8 Color of status lines
       Home Start of files
       End  End of file
       W   Wrap long lines on/off
       P   Printing on/off
       7,8 Strip or leave hi-bit
       S   Save defaults

       ESC Return to file

Command▶                                  Keys:↑↓←→ PgUp PgDn ESC=Exit F1=Help
```

Figure A-7 Screen Report Help

B. Using SPAN

1. Main Menu

Each SPAN session begins at the **Main** menu. (Figures A-3, A-8) It is the highest level in the menu hierarchy, and therefore the focal point of all of SPAN's menus. The commands on SPAN's **Main** menu reflect the program's structure. It includes the following six selections.

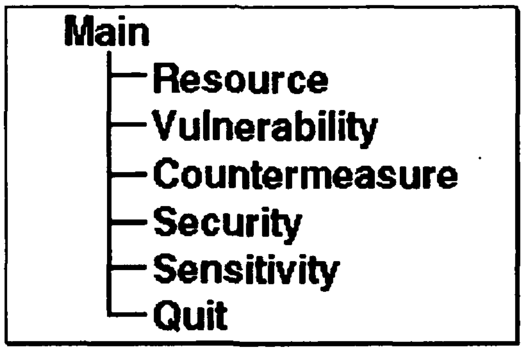


Figure A-8 Main Menu Structure

a. Resource

The Resource selection allows the entry of location and resource information. You also may generate reports based on location, resource type, resource value, or a summary report of all resources in the organization.

b. Vulnerability

The Vulnerability selection provides five major functions.

1. Update the system's list of possible threats by adding, modifying or deleting potential threats.

2. Identify and select those threats that apply to the entire organization, a specific location, a certain type or IS resources, or to a particular resource.

3. Assign a perceived vulnerability level to any resource according to the specific threats and their probability or occurrence. Vulnerability levels are assigned on a ten point scale (one, extremely low vulnerability; ten, extremely high vulnerability).

4. Revise and update threat and vulnerability data associated with the entire organization, a specific location, a certain type of IS resources, or a particular resource.

5. Produce reports that exhibit locations, types of resources or specific resources that are most vulnerable to threats. This vulnerability representation aims to define where the greatest exposures exist.

c. Countermeasure

The Countermeasure selection allows the user to identify a profile of existing countermeasures. Reports can be generated by location, resource criticality, threat or specific countermeasure.

d. Security

The Security selection correlates each vulnerability exposure to protection affected by existing countermeasures. An effectiveness score based on a ten point scale (one, ineffective; ten, highly effective) is incorporated into SPAN and allows the assessment of an effectiveness level of existing countermeasures. This permits the following.

1. Identify locations, resource types or resources with potentially inadequate countermeasures in place.
2. Rank locations and resources warranting further study or countermeasure funding.
3. Approximate the effectiveness of proposed countermeasures.

Another function included in this selection is security plan formulation. This feature provides the ability to produce a draft of an IS security plan as a product of the security analysis process.

e. Sensitivity

The Sensitivity selection allows the user to perform further analysis through "what if" modeling. These scenarios are created by entering additional data elements or parameters to the existing database and examining their impact on the system's outputs. The product of this analysis can be presented on the screen or sent to the printer. The changes performed during these scenarios do not alter SPAN's database.

f. Quit

This selection is used to quit SPAN and return to DOS. The final screen asks if you are sure you want to leave the program, and allows the continuation of the current SPAN session if so desired.

2. Resource Menu

The structure and format of the **Resource** menu are found in Figures A-9 and A-10.

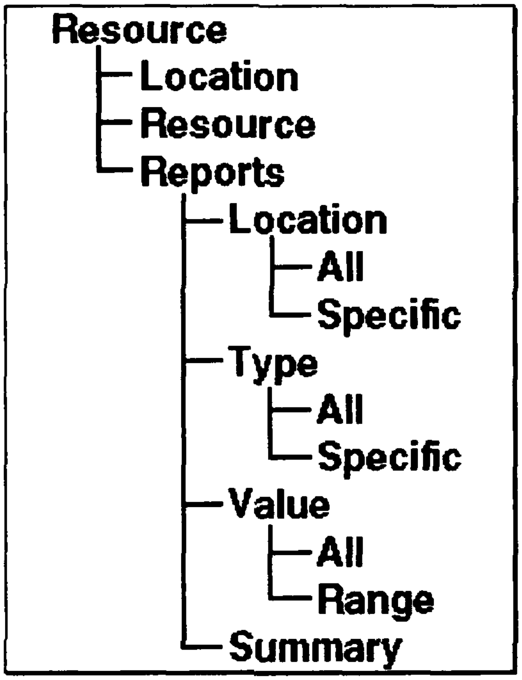


Figure A-9 Resource Menu Structure

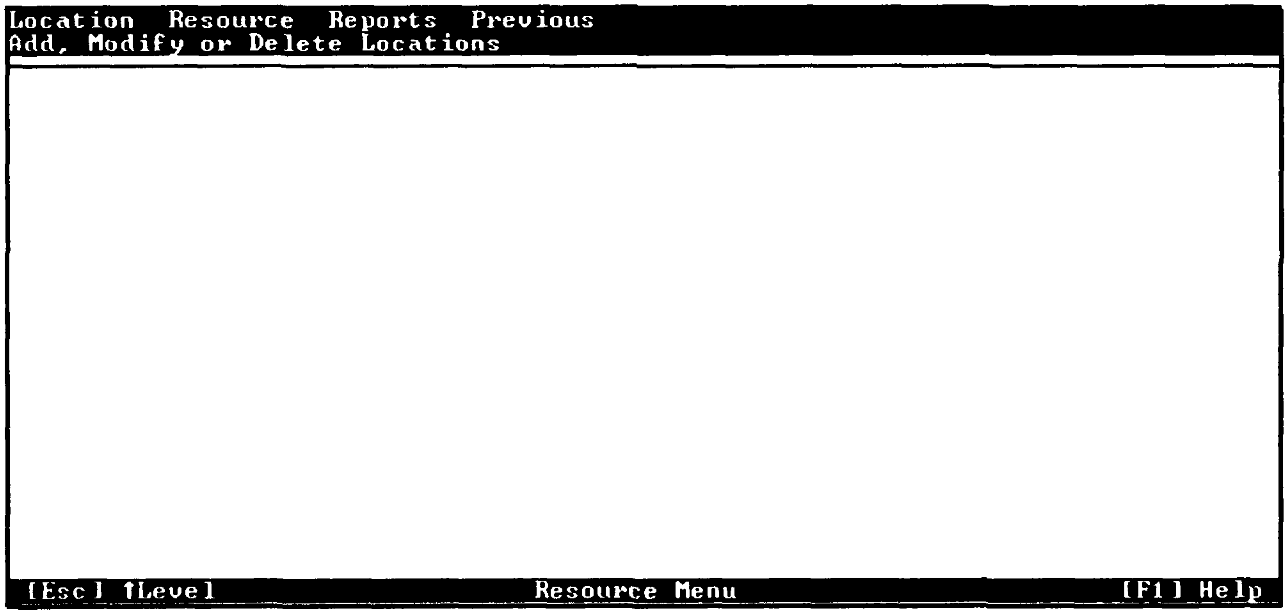
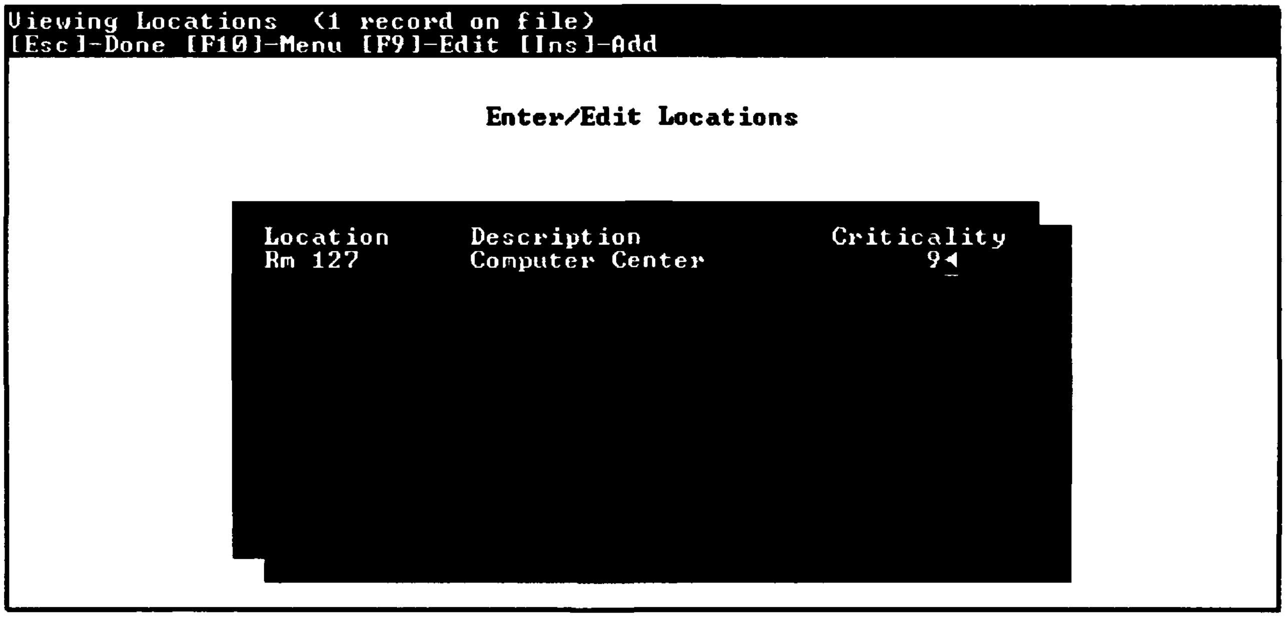

Location Resource Reports Previous
Add, Modify or Delete Locations
[Esc] ↑Level
Resource Menu
[F1] Help

Figure A-10 Resource Menu

a. Location

This selection should be the first one made during your initial SPAN session. It provides the foundation for all of SPAN's data.

The ***location*** form requires the entry of information in three fields. The first entry is under the heading of *location*. Enter a name or number that uniquely describes a location in your organization. A location is any room, office or designated area that contains IS resources. (Figure A-11)



```
Viewing Locations  (1 record on file)
[Esc]-Done [F10]-Menu [F9]-Edit [Ins]-Add

                     Enter/Edit Locations

       Location      Description            Criticality
       Rm 127        Computer Center              9◄
```

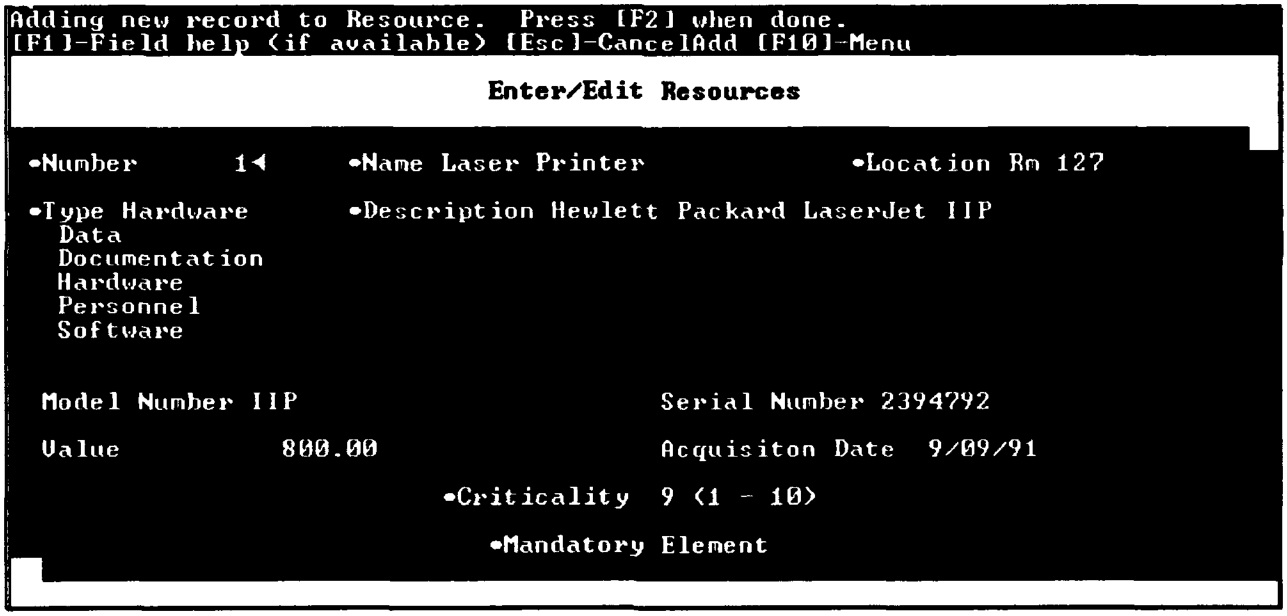
Figure A-11 Location Form

The next information entered is in the *description* field. The location's description may be up to twenty characters in length. A typical entry is a few words describing the location or the official title of the location.

The final field is *Criticality*. Criticality is a numerical representation of the importance of the location to the organization. A location with a high criticality is essential to the daily operations or mission of the organization. A location with a low criticality has little or no effect on the operations or mission of the organization, while a location with a high criticality is essential to the organization. The location criticality is a subjective value that should consider all computing resourccs in the location. A location with a high criticality value will normally contain computing resources of high criticality. The *Criticality* field accepts a number from one to ten.

b. Resource

The Resource selection maintains a database of the organization's IS resources. There are a six mandatory fields on this form, each marked by "•." This form may not be exited if any of the mandatory fields contain an invalid entry or have been left blank. (Figure A-12)



```
Adding new record to Resource.  Press [F2] when done.
[F1]-Field help (if available) [Esc]-CancelAdd [F10]-Menu

                          Enter/Edit Resources

 •Number       1◄     •Name Laser Printer            •Location Rm 127

 •Type Hardware       •Description Hewlett Packard LaserJet IIP
   Data
   Documentation
   Hardware
   Personnel
   Software

  Model Number IIP                    Serial Number 2394792

  Value          800.00               Acquisiton Date  9/09/91

                          •Criticality  9 (1 - 10)

                            •Mandatory Element
```

Figure A-12 Resource Form

The first field on the ***Resource*** form is *Number.* SPAN automatically assigns a unique number to each resource added to the database. The value assigned in *Number* may not be changed.

The *Name* field is designed to accept a short description (twenty characters) of the IS resource. A typical entry is a general description of the resource, such as "Laser Printer" or "Network Server." A longer detailed description must be entered in the *Description* field. Both entries are mandatory.

The entry made in the *Location* field must correspond with a location entered on the ***Location*** form. Any entry that does not match a previously entered location will be rejected. If no locations have been entered in SPAN's database, you may not enter a new resource. Pressing **F1** while the cursor is on the *Location* field will bring up a list of all locations in SPAN's database. You may press **Esc** to leave this list, or move the cursor to the desired location and press **F2**. The desired location will be placed in the *Location* field on the ***Resource*** form.

You must now determine the resource type. SPAN recognizes five resource types; Data, Documentation, Hardware, Personnel and Software. The *Type* field accepts only the characters that are highlighted on the form. The remaining characters are automatically entered by SPAN. For example, if you press **d** and **o**, SPAN will enter "Documentation" in the *Type* field.

The final mandatory field is *Criticality*. The default value for the level of criticality is equal to the one assigned to the specific location. When a location is entered in the *Location* field, the location's criticality is automatically entered in the *Criticality* field. You may change this value to any number between one and ten to reflect the criticality of the individual resource.

The remaining fields on the ***Resource*** form are not mandatory, but it is highly recommended that they are used. Many of SPAN's reports depend on information found in these fields. These fields include *Model Number, Serial Number, Acquisition Date* and *Value*.

c. Reports

(1) Location. The first of SPAN's resource reports is the ***Location*** report. When this option is selected, you will be presented with the option of producing a report generated by **A**ll locations or a **S**pecific location. If you select **S**pecific, you will be presented with a screen asking for the name of the desired location. You must enter the name of the location exactly as it was entered on the ***Location*** form.

The ***Location*** report exhibits all resources that are assigned to each location. If **A**ll was selected, the report will exhibit all locations and the resources found in each. The **S**pecific option will exhibit all resources found in a designated location. As with all of SPAN's reports, the ***Location*** report may be sent to the printer or screen.

(2) Type. This selection generates resource reports grouped by resource type. Like the ***Location*** report, the ***Type*** report may be generated for **A**ll or **S**pecific records.

(3) Value. The **V**alue selection generates reports based on the dollar value of resources. Selecting **A**ll will produce a report of all resources in the organization, sorted by their value. The **R**ange selection allows you to enter the lower and upper values of a desired range. SPAN will generate the report based on your selected range.

(4) Summary. The last of the report selections generates reports that feature all resources in the organization. Resources are presented in numerical order and exhibit all available information.

d. Previous

The **P**revious selection exits the current menu level and returns to previous level. This option is found on most of SPAN's menus.

3. Vulnerability Menu

The structure and format of the **Vulnerability** menu are found in Figures A-13 and A-14.

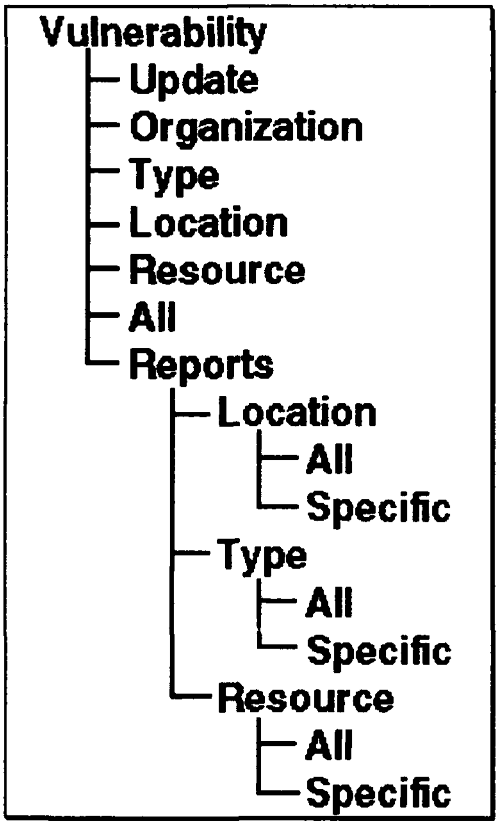
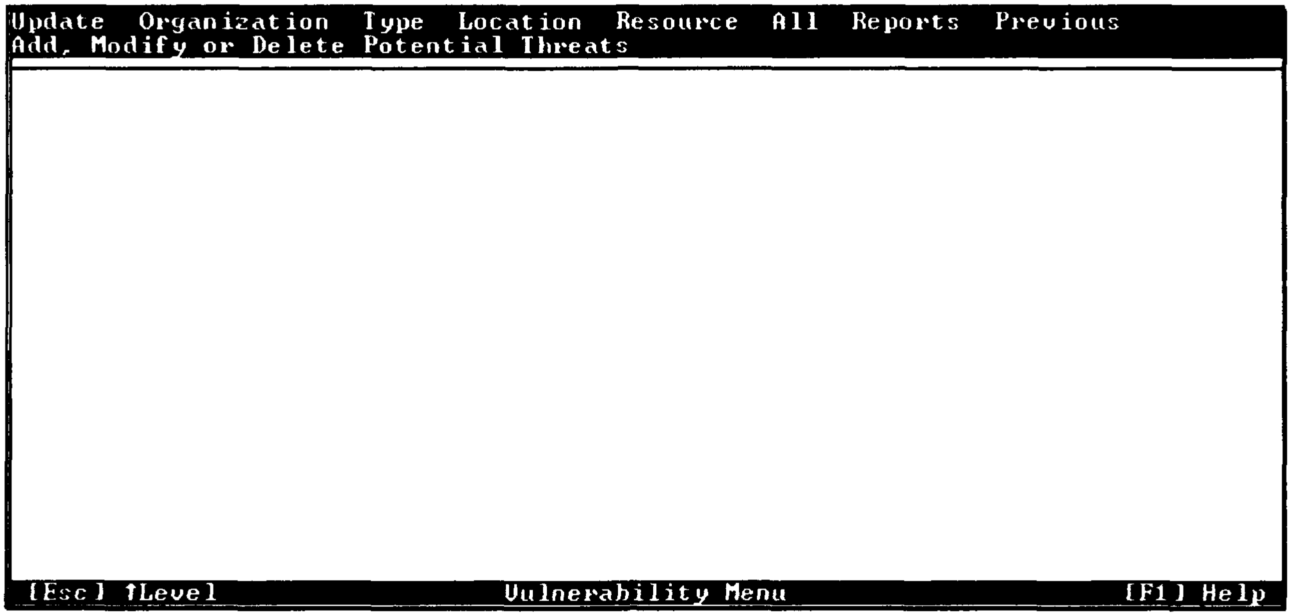


Figure A-13 Vulnerability Menu Structure

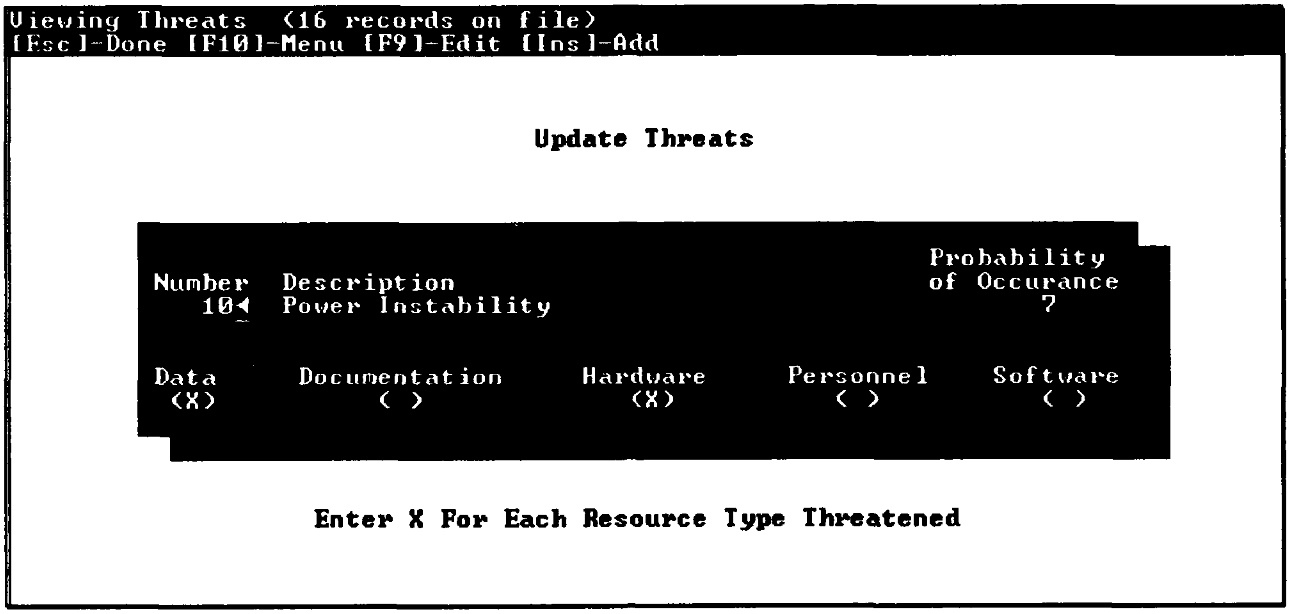

Update Organization Type Location Resource All Reports Previous
[Esc] ↑Level
Vulnerability Menu
[F1] Help

Add, Modify or Delete Potential Threats

Figure A-14 Vulnerability Menu

a. Update

The Update selection allows the addition, modification or deletion of potential threats. (Figure A-15) SPAN's database contains many common threats that are applicable to most organizations. You may add to this database by entering additional threats.



```
Viewing Threats  (16 records on file)
[Esc]-Done [F10]-Menu [F9]-Edit [Ins]-Add

                         Update Threats

                                                    Probability
     Number   Description                           of Occurance
       10◄    Power Instability                           7

     Data      Documentation     Hardware     Personnel     Software
     (X)           ( )             (X)           ( )           ( )

              Enter X For Each Resource Type Threatened
```

Figure A-15 Update Form

Threat records are automatically numbered in consecutive order, in the same manner as SPAN's Resource records. The number appears in the *Threat Number* field. This field may not be edited.

The *Description* field contains a description of up to 40 characters in length. Each new threat will require an entry in this field.

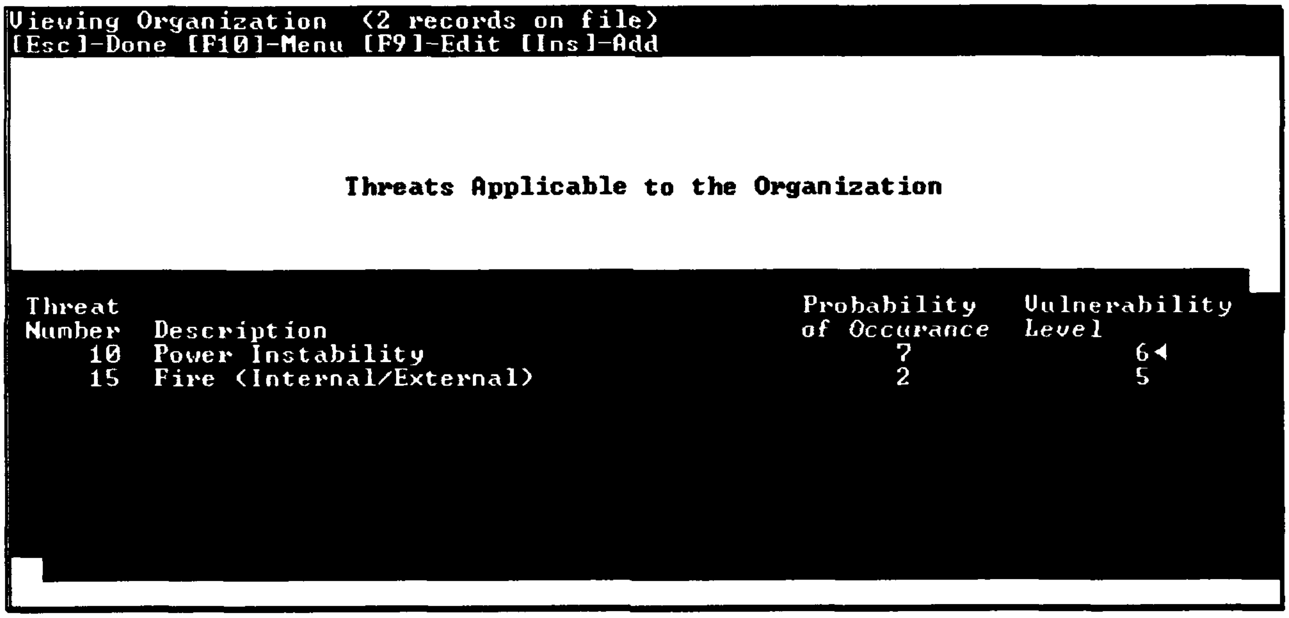
The next field holds the *Probability of Occurrence.* The *Probability of Occurrence* represents the relative probability of the threat occurring at your organization. Accepted values are between one and ten, where one represents a very low probability and ten means that the threat is likely to occur.

The bottom row of the form displays each available resource types. You must enter **X** below each resource type affected by the threat. At least one resource type must be selected.

SPAN correlates each newly added threat with all countermeasures that are effective against the threat. Many of SPAN's operations depend on accurate effectiveness values. After adding a threat to SPAN's database, you will be given the option of updating the effectiveness values for the new threat and existing countermeasures. Select Continue to update the effectiveness values for the new threat. If Quit is selected, you will not be able to proceed with security plan formulation until you have updated all effectiveness values.

b. Organization

This is the first form on which threats are assigned. Threats entered on this form are those that apply to the entire organization, and will be assigned to every resource in the organization. (Figure A-16)



```
Viewing Organization  (2 records on file)
[Esc]-Done [F10]-Menu [F9]-Edit [Ins]-Add

                     Threats Applicable to the Organization

Threat                                              Probability   Vulnerability
Number   Description                                of Occurance  Level
    10   Power Instability                                7              6◄
    15   Fire (Internal/External)                         2              5
```

Figure A-16 Organization Form

The first field is *Threat Number*. Only valid threat numbers may be entered. Pressing **F1** will display a list of all valid threats. You may use the arrow keys to though the list and locate a specific threat. Press **Esc** to exit the list, or press **F2** while the cursor is on a threat number to enter the threat on the form.

The *Description* field will automatically be filled with the description of the chosen threat. This description is found on the ***Update*** form. You may not edit the

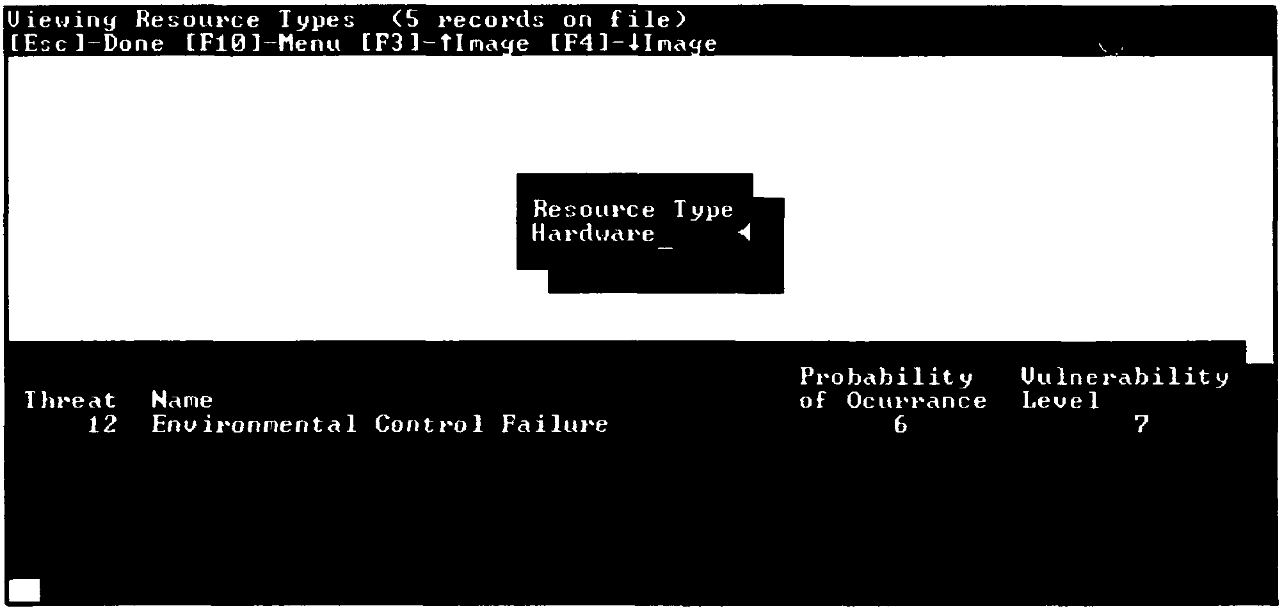
Description on any of the assignment forms. Editing may only be performed during the Update procedure.

The *Probability of Occurrence* will be filled with the value assigned during the Update procedure. This field may be updated to reflect the probability that this threat will occur to the entire organization.

The last field contains the *Vulnerability Level.* This is one of the most important entries that you will make in SPAN's database. Vulnerability represents the impact of an occurrence of a threat on the organization's ability to function. A ten point scale is used, where one represents no impact on the organization's ability to function, and ten denotes a situation where the organization is unable to carry out its primary mission or function.

c. Type

The **Type** selection allows threats to be assigned to resource types. (Figure A-17) Threats assigned on this form will be associated with each resource of the specified type. SPAN will not allow the assignment of a threat if it does not apply to the specified resource type.



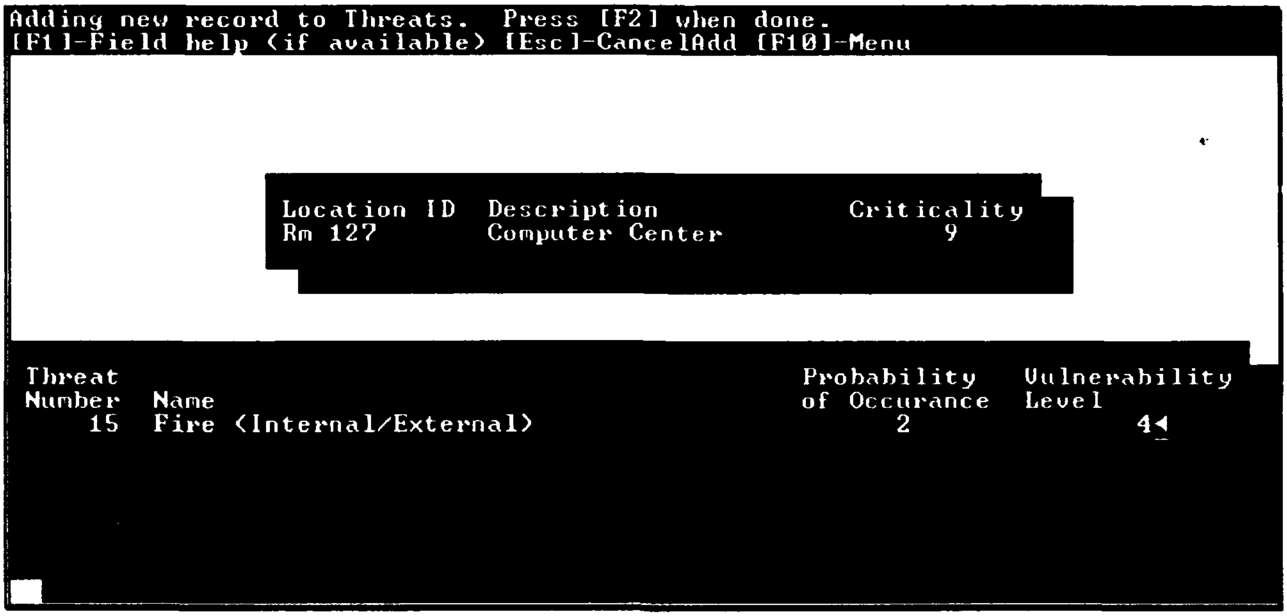
```
Viewing Resource Types  (5 records on file)
[Esc]-Done [F10]-Menu [F3]-↑Image [F4]-↓Image

                    Resource Type
                    Hardware_     ◄

                                             Probability      Vulnerability
Threat  Name                                 of Ocurrance     Level
   12   Environmental Control Failure            6                  7
```

Figure A-17 Type Form

This is the first of SPAN's forms that presents data in two images. The top image on the form displays each available resource type. This field may not be edited. The bottom image allows the entry and modification of threats. The fields and procedures are identical with those of the ***Organization*** form. Any changes made to the *Probability of Occurrence* or *Vulnerability Level* will override previously entered values. This is an example of the hierarchy in SPAN's database. Entries made at lower, more detailed levels override those made at higher, more general levels.

d. Location

This selection allows the assignment of threats to locations. (Figure A-18) A threat assigned to a location is also assigned to every applicable resource in that location.



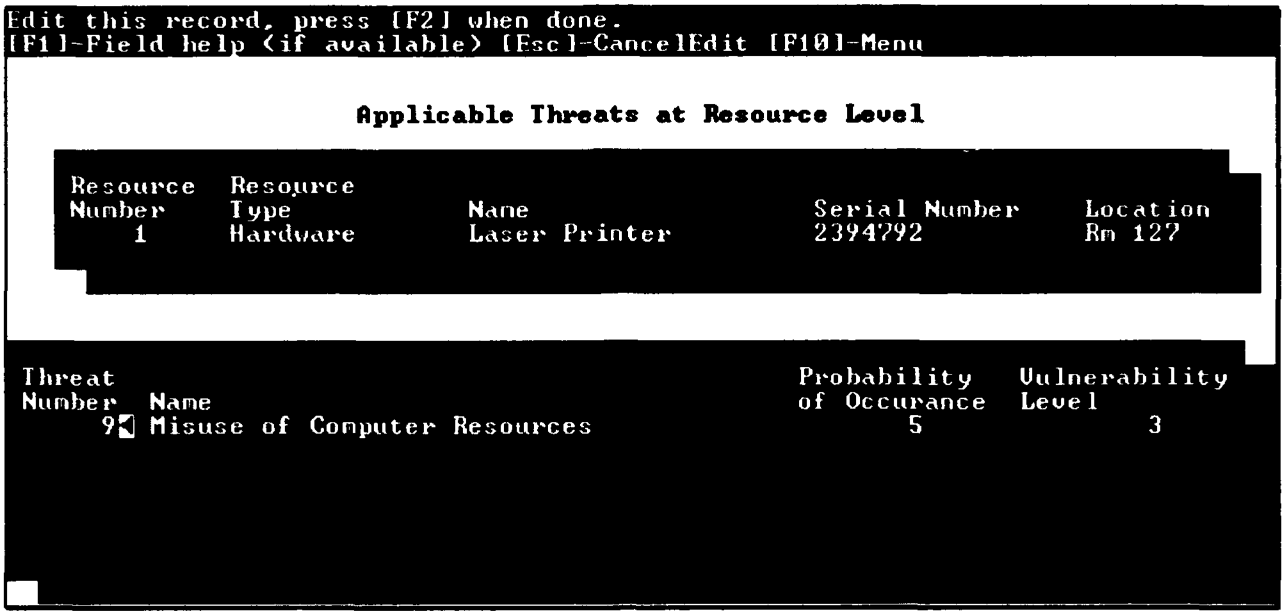
```
Adding new record to Threats.  Press [F2] when done.
[F1]-Field help (if available) [Esc]-CancelAdd [F10]-Menu

                 Location ID  Description          Criticality
                 Rm 127       Computer Center           9

 Threat                                          Probability     Vulnerability
 Number   Name                                   of Occurance    Level
    15    Fire (Internal/External)                    2                4
```

Figure A-18 Location Form

The upper image contains each location that has been entered into SPAN's database. The lower image contains the data fields for threats. The fields and procedures are identical with the ***Organization*** and ***Type*** forms.

e. Resource

The **R**esource selection allows the assignment of threats to individual resources. (Figure A-19) This is the most detailed level of the vulnerability database. Information entered at this level will override all previously entered data.



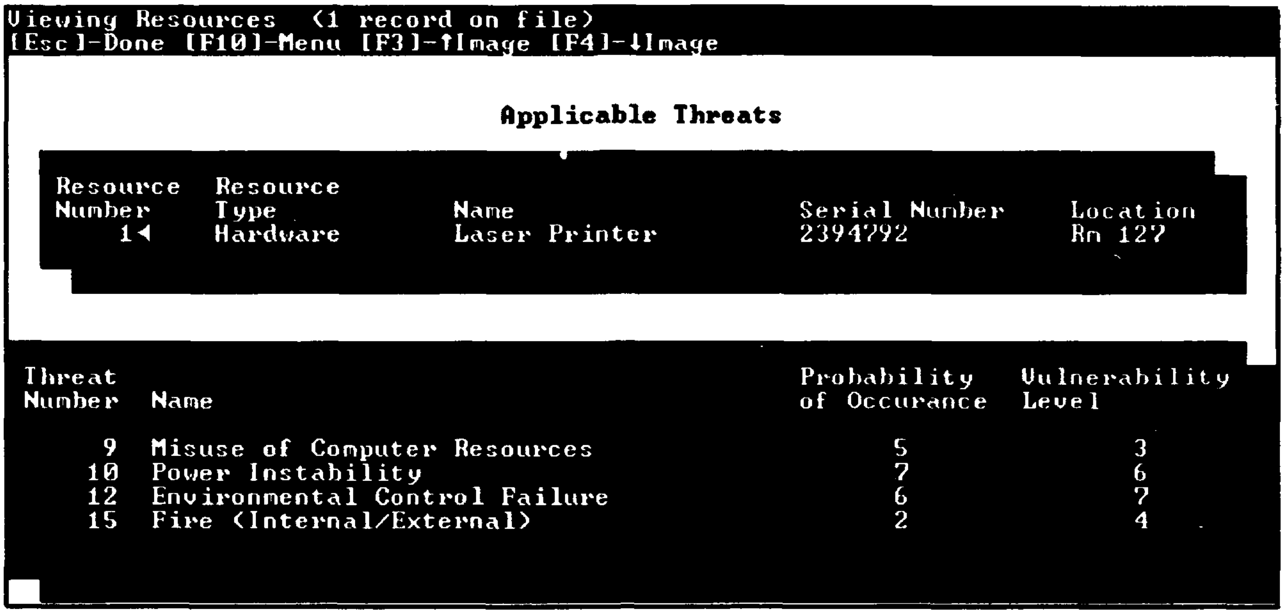
```
Edit this record, press [F2] when done.
[F1]-Field help (if available) [Esc]-CancelEdit [F10]-Menu

                    Applicable Threats at Resource Level

  Resource   Resource
  Number     Type            Name                      Serial Number    Location
     1       Hardware        Laser Printer             2394792          Rm 127

Threat                                                  Probability   Vulnerability
Number  Name                                            of Occurance  Level
      9 Misuse of Computer Resources                         5              3
```

Figure A-19 Resource Form

This form follows the same pattern as the previous threat assignment forms. The upper image contains all of the resources that have been entered in SPAN's database. The lower image contains the data fields for threats. The fields and procedures are identical with those found on the ***Organization***, ***Type***, and ***Location*** forms.

f. All

The All selection allows the viewing of all resources in SPAN's database and their associated threats. (Figure A-20) This includes threats assigned at the organization, resource type and location levels, as well as the threats assigned directly to resources. No editing may be performed on this form.



```
Viewing Resources  (1 record on file)
[Esc]-Done [F10]-Menu [F3]-↑Image [F4]-↓Image

                          Applicable Threats

 Resource  Resource
 Number    Type        Name                 Serial Number   Location
    1◄     Hardware    Laser Printer        2394792         Rm 127

Threat                                      Probability   Vulnerability
Number  Name                                of Occurance  Level

     9  Misuse of Computer Resources             5              3
    10  Power Instability                        7              6
    12  Environmental Control Failure            6              7
    15  Fire (Internal/External)                 2              4
```

Figure A-20 All Form

g. Reports

(1) Location. The first of SPAN's vulnerability reports is the ***Location*** report. When this selection is chosen you will be presented with the option to produce a report generated by All locations or a Specific location. If Specific is selected, you will be presented with a screen asking for the name of the desired location. You must enter the name of the location exactly as it was entered on the ***Location*** form.

The ***Location*** reports exhibit all threats that are assigned to locations. If All is selected, the report will exhibit all locations and the threats assigned to each. The location that is most vulnerable to threats will be listed first, followed by the remaining locations in descending order of vulnerability. The Specific option will exhibit all threats assigned to a designated location. Like all of SPAN's reports, the ***Location*** report may be sent to the printer or screen.

(2) Type. This selection generates vulnerability reports grouped by resource type. The report exhibits all threats assigned to resource types, and can be generated for All or Specific resource types.

(3) Resource. The **R**esource selection produces vulnerability reports exhibiting threats assigned to resources. ***Resource*** reports can be generated for **A**ll or **S**pecific resources.

4. Countermeasure Menu

The structure and format of the **Countermeasure** menu are found in Figures A-21 and A-22.

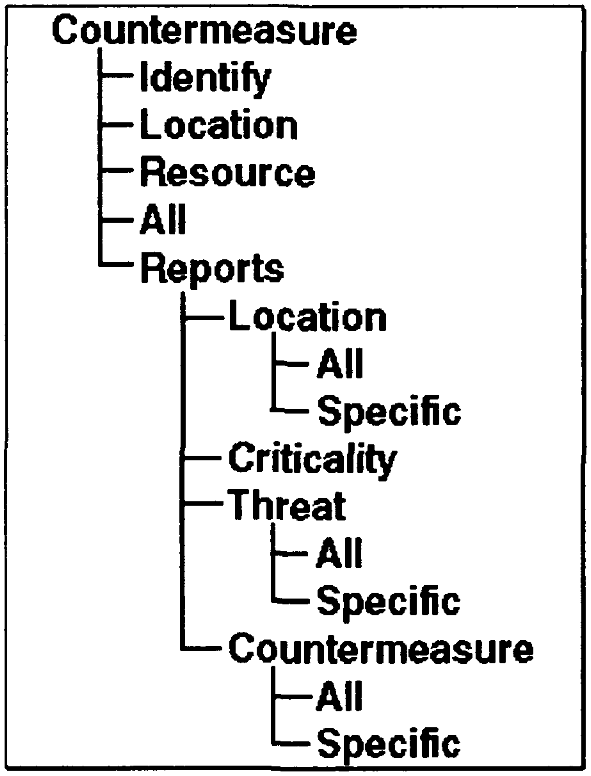


Figure A-21 Countermeasure Menu Structure

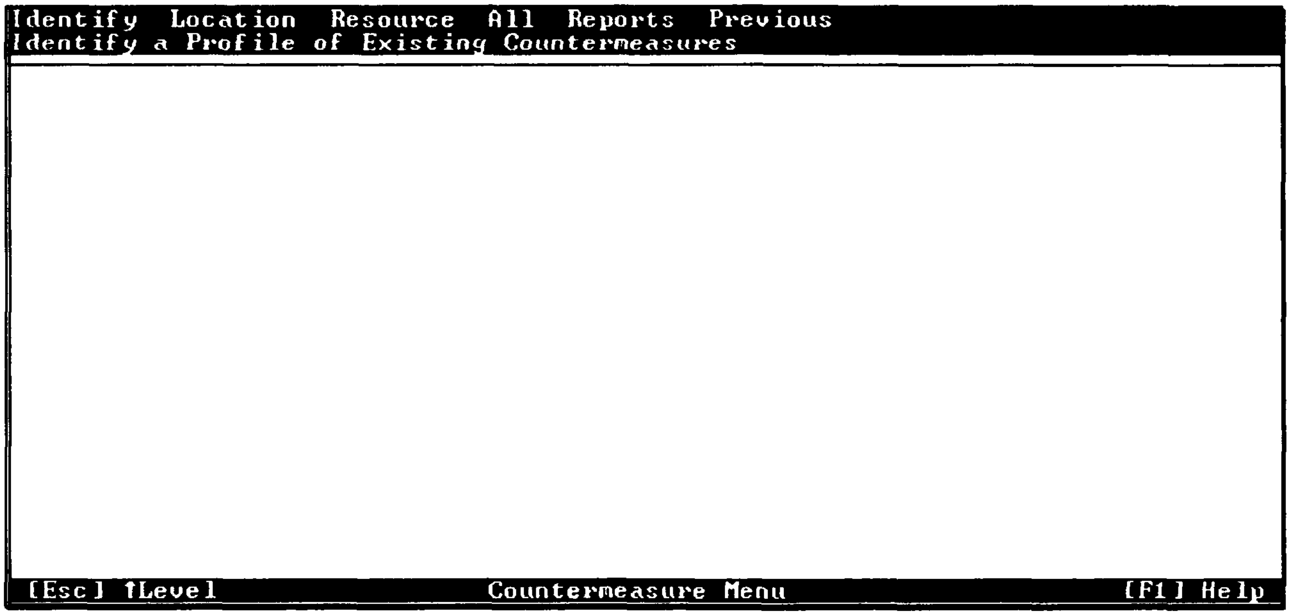
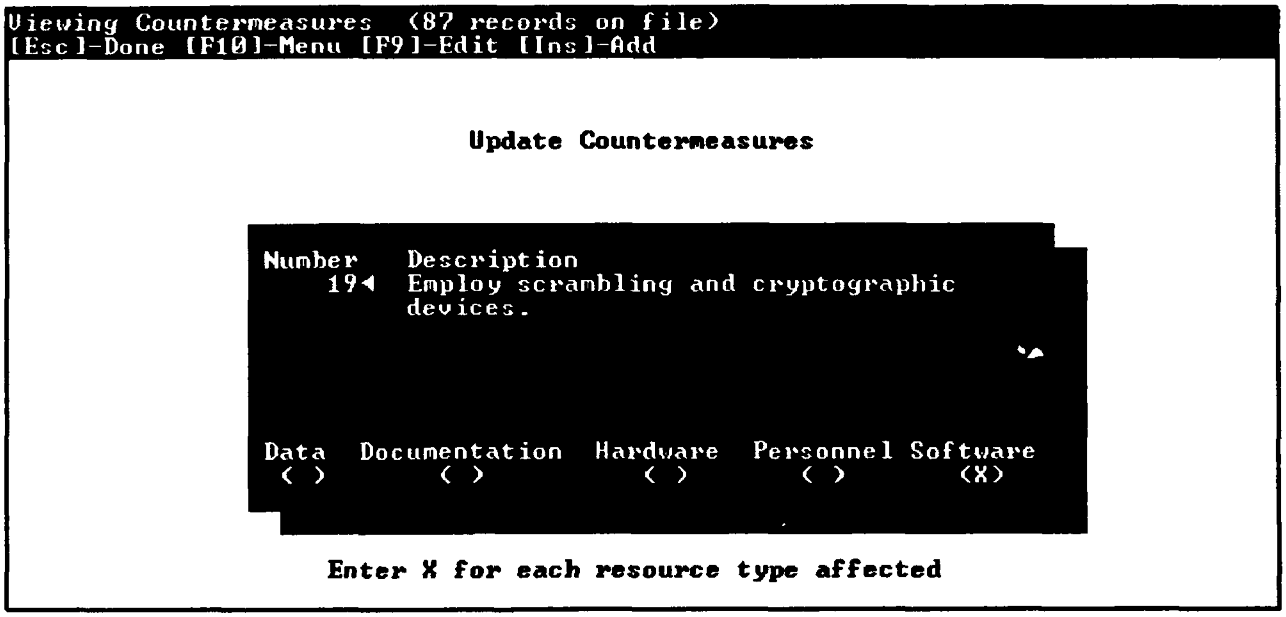

Identify Location Resource All Reports Previous
Identify a Profile of Existing Countermeasures
[Esc] ↑Level
Countermeasure Menu
[F1] Help

Figure A-22 Countermeasure Menu

a. Identify

The Identify selection enables the identification of a profile of existing countermeasures. (Figure A-23) Countermeasures may be added, modified or deleted on this form. SPAN's database contains several common countermeasures that can be implemented by most organizations. You may add to this database by entering additional countermeasures.



```
Viewing Countermeasures  (87 records on file)
[Esc]-Done [F10]-Menu [F9]-Edit [Ins]-Add

                     Update Countermeasures

         Number   Description
             19◄  Employ scrambling and cryptographic
                  devices.

         Data  Documentation  Hardware  Personnel Software
          ( )       ( )          ( )       ( )       (X)

              Enter X for each resource type affected
```

Figure A-23 Identify Form

Countermeasure records are automatically numbered in consecutive order. The countermeasure number appears in the *Number* field and may not be edited.

The *Description* field contains a detailed description of the countermeasure. This description can be up to 240 characters in length. Each new countermeasure will require an entry in this field.

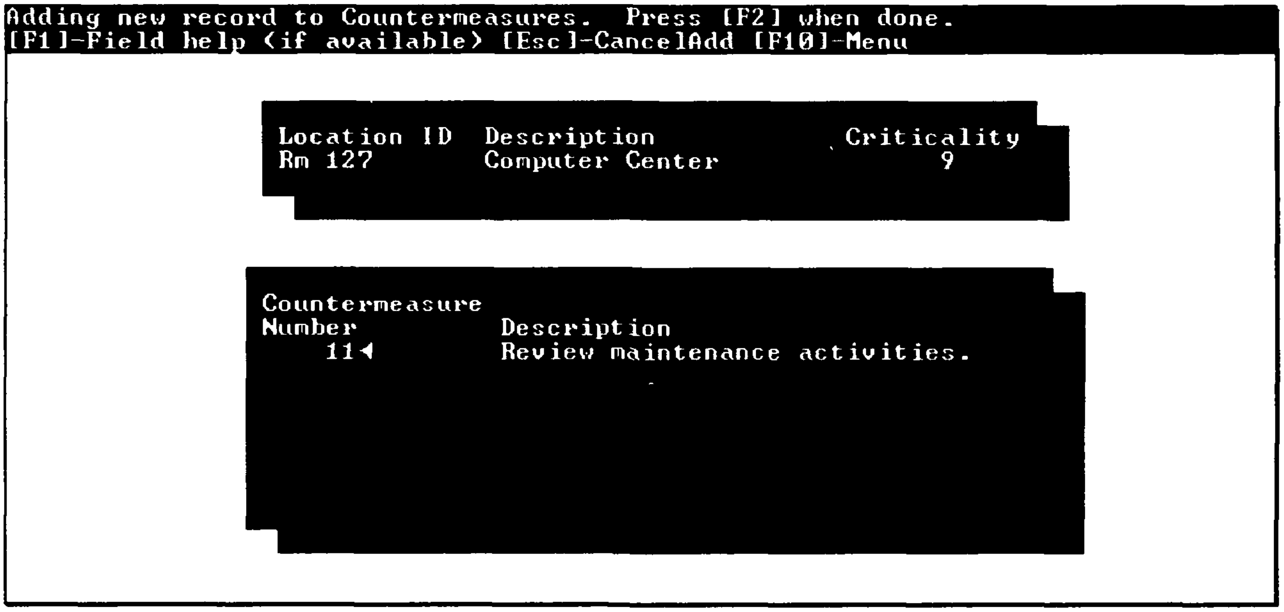
The bottom row of the form displays each available resource type. You must enter **X** below each resource type affected by the countermeasure. At least one resource type must be selected.

Many of SPAN's operations depend on accurate effectiveness values. SPAN correlates each newly added countermeasure with all applicable threats. After adding a countermeasure to SPAN's database, you will be presented with a screen giving you the option of updating the effectiveness values for the new countermeasure and existing threats. You have the option to Continue or Quit. Select Continue to update the effectiveness values for the new countermeasure. If you select Quit, you will not be able to proceed with security plan formulation until you have updated all effectiveness values.

If an existing countermeasure is edited, all instances of the countermeasure will be deleted. If the countermeasure has been assigned to any locations or resources, all assignments will be removed.

b. Location

This selection allows the assignment of countermeasures to locations. A countermeasure assigned to a location is also assigned to every applicable resource in that location. (Figure A-24)



```
Adding new record to Countermeasures.  Press [F2] when done.
[F1]-Field help (if available) [Esc]-CancelAdd [F10]-Menu

        Location ID  Description          Criticality
        Rm 127       Computer Center           9

        Countermeasure
        Number          Description
            11◄         Review maintenance activities.
```

Figure A-24 Location Form

The upper image contains every location that has been entered into SPAN's database. The lower image contains the data fields for countermeasures.

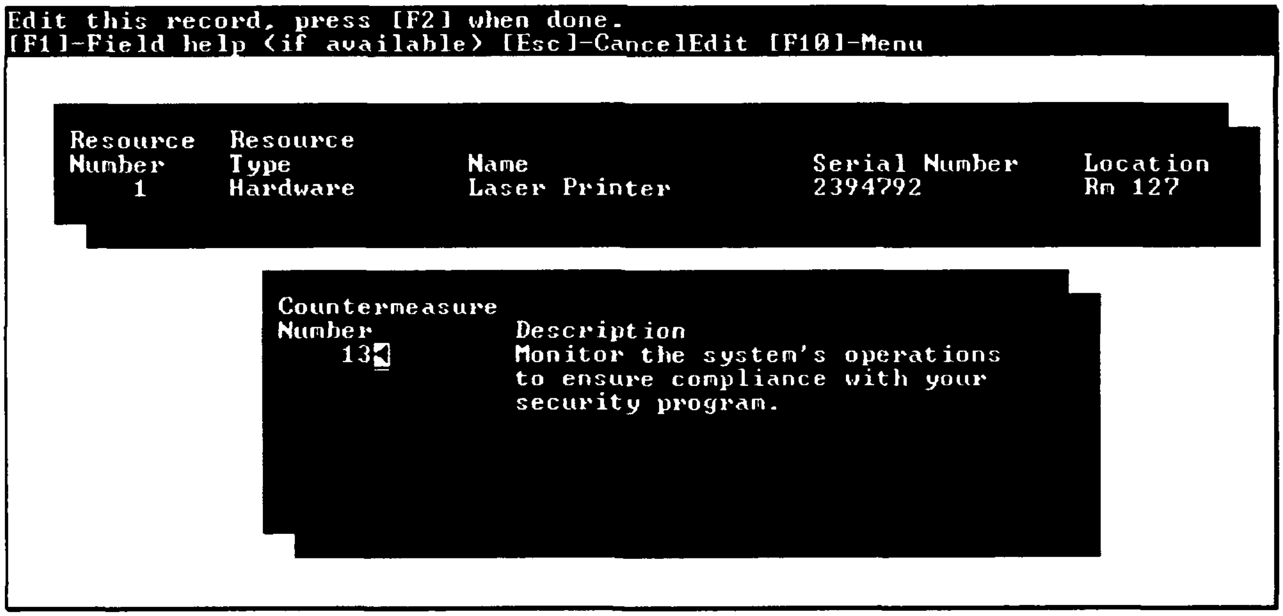
The first countermeasure field is *Countermeasure Number.* Pressing **F1** will display a list of all valid countermeasures. You may use the arrow keys to scroll through the list to locaie a specific countermeasure. Press **Esc** to exit the list, or press **F2** while the cursor is on a countermeasure number to enter that countermeasure on the form.

The *Description* field will automatically be filled with the description of the chosen countermeasure. The description is found on the ***Identify*** form. You may not edit the countermeasure description on either of the assignment forms, it may only be done as part of the Identify procedure.

The bottom line displays the resource types affected by the countermeasure. This information is also taken from the ***Identify*** form.

c. ***Resource***

The **R**esource selection allows the assignment of countermeasures to individual resources. (Figure A-25) Countermeasures entered on this form should be those that have been implemented for single resources. If a countermeasure has been implemented for all resources in a location, the countermeasure should be entered on the ***Location*** form.



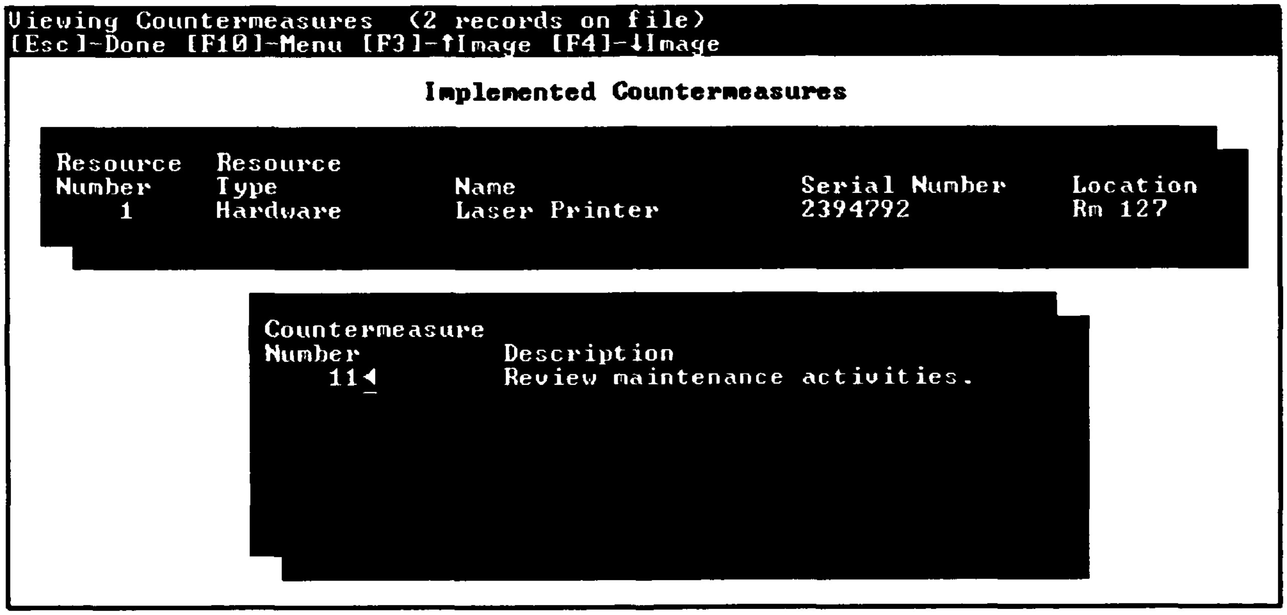
```
Edit this record, press [F2] when done.
[F1]-Field help (if available) [Esc]-CancelEdit [F10]-Menu

Resource  Resource
Number    Type       Name            Serial Number   Location
   1      Hardware   Laser Printer   2394792         Rm 127

Countermeasure
Number          Description
    13          Monitor the system's operations
                to ensure compliance with your
                security program.
```

Figure A-25 Resource Form

This form follows the same format as the ***Location*** form. The upper image contains all resources entered in SPAN's database, and the lower image contains the data fields for countermeasures.

d. ***All***

The All selection allows the viewing of all resources in SPAN's database and their associated countermeasures. (Figure A-26) This includes countermeasures implemented for locations as well as the countermeasures implemented for individual resources. No editing may be performed on this form.



```
Viewing Countermeasures  (2 records on file)
[Esc]-Done [F10]-Menu [F3]-↑Image [F4]-↓Image

                     Implemented Countermeasures

 Resource  Resource
 Number    Type           Name                Serial Number    Location
    1      Hardware       Laser Printer       2394792          Rm 127


             Countermeasure
             Number        Description
                11◄        Review maintenance activities.
```

Figure A-26 All Form

e. ***Reports***

(1) Location. The Location selection allows the user to produce countermeasure reports by location. Reports can be generated for All locations or Specific locations. If Specific is selected, you will be presented with a screen asking for the name of desired location. You must enter the name of the location exactly as it was entered on the Location form.

The ***Location*** report will exhibit all countermeasures that are implemented for locations. If **All** is selected, the report will exhibit all locations and the countermeasures implemented for each. The **Specific** option will exhibit all countermeasures implemented for a designated location. Like all of SPAN's reports, the ***Location*** report may be sent to the printer or screen.

(2) Criticality. This selection generates countermeasure reports based on resource criticalities. The organizations' resources are sorted by criticality and listed with their implemented countermeasures.

(3) Threat. The **Threat** selection produces countermeasure reports based on threats to the organization. Each threat is presented with a list of implemented countermeasures. Reports may be generated for **All** or **Specific** threats.

(4) Countermeasure. The ***Countermeasure*** report lists all countermeasures that have been implemented in the organization, grouped with a list of applicable threats. Reports may be generated for **All** or **Specific** countermeasures.

5. Security Menu

The structure and format of the **Security** menu are found in figures A-27 and A-28.

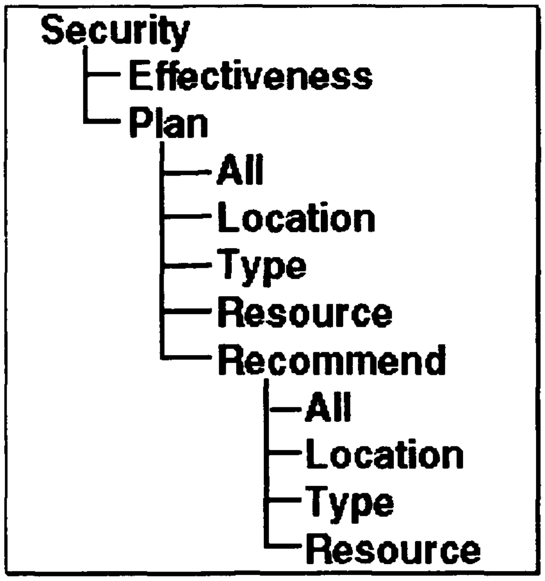
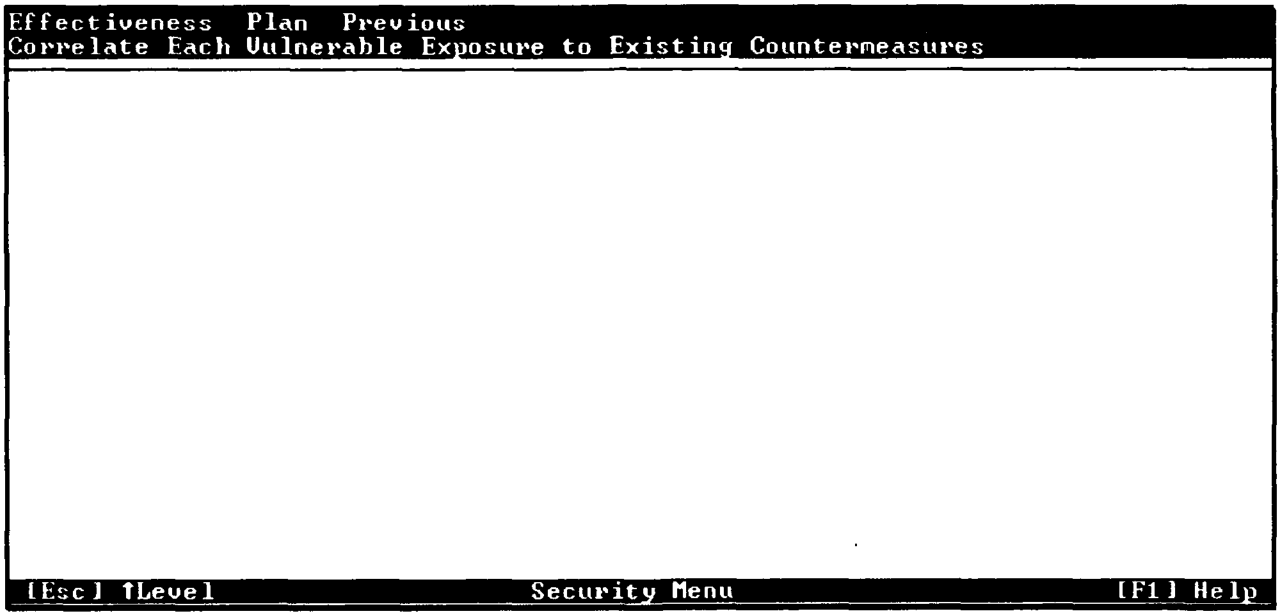


Figure A-27 Security Menu Structure

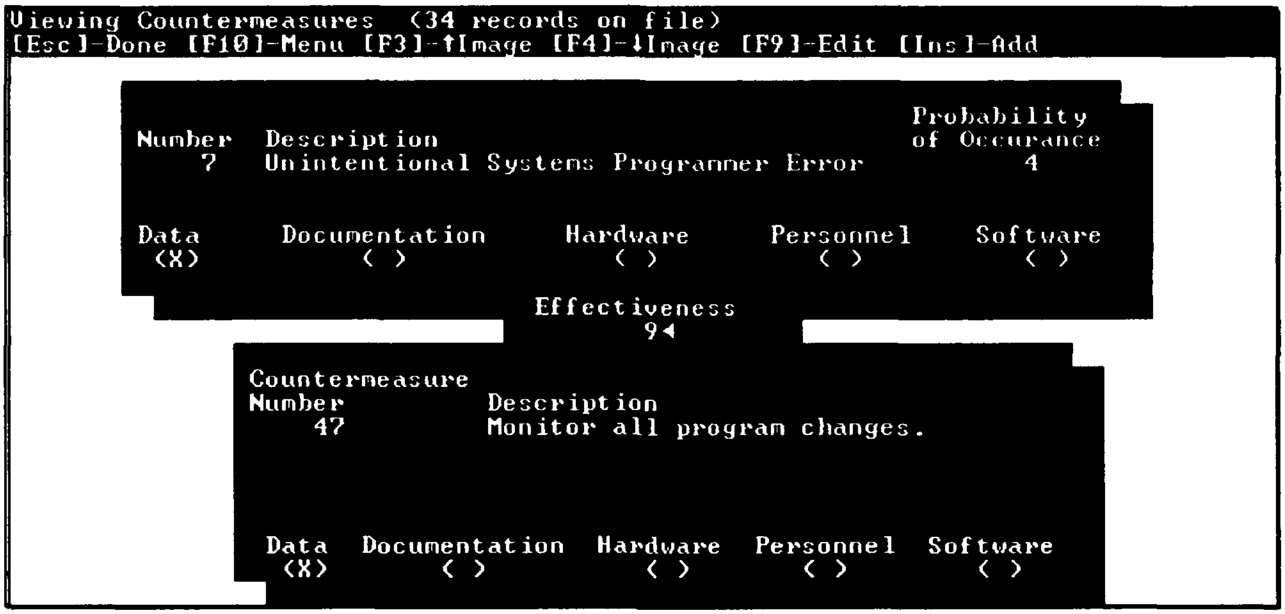


```
Effectiveness  Plan  Previous
Correlate Each Vulnerable Exposure to Existing Countermeasures

 [Esc] ↑Level                      Security Menu                      [F1] Help
```

Figure A-28 Security Menu

a. *Effectiveness*

The Effectiveness selection correlates each vulnerable exposure to protection affected by existing countermeasures. (Figure A-29) Effectiveness is scored on a ten point scale (one, ineffective; ten, highly effective).



```
Viewing Countermeasures  (34 records on file)
[Esc]-Done [F10]-Menu [F3]-↑Image [F4]-↓Image [F9]-Edit [Ins]-Add

                                                                Probability
  Number  Description                                           of Occurance
     7    Unintentional Systems Programmer Error                     4

  Data      Documentation      Hardware      Personnel      Software
  (X)           ( )               ( )           ( )            ( )

                              Effectiveness
                                    9◄

        Countermeasure
        Number          Description
           47           Monitor all program changes.



         Data   Documentation   Hardware   Personnel   Software
          (X)        ( )           ( )        ( )         ( )
```

Figure A-29 Effectiveness Form

Each assigned threat is matched with every implemented countermeasure that is effective against the threat. SPAN's initial database contains effectiveness values for all countermeasures and threats. You must update the effectiveness values for all threats and countermeasures that have been added or changed. All effectiveness values must be entered before proceeding with security plan formulation.

The upper image contains each threat in SPAN's database. The lower image consists of two parts. The bottom part of the image contains countermeasure data, and the middle box contains the effectiveness value. The *Effectiveness* field is the only one that may be edited on this form.

b. Plan

The Plan selection creates draft security plans. You may produce a plan based on the existing countermeasures, or allow SPAN to recommend a set of countermeasures. This process is highly dependent on the effectiveness values entered on the effectiveness form. If any of these values are missing, SPAN will alert you before be for allowing you to proceed with security plan formulation.

The **Plan** selection will cause SPAN immediately to begin a check of all threats and countermeasures, searching for invalid or missing parameters. This process may take a minute or more to complete, depending on the number of threats and countermeasures in SPAN's database and the speed of your machine. If SPAN finds a missing effectiveness value, you will be presented with a screen giving you the option of updating the missing effectiveness values. You have the option to Continue or Quit. Select Continue to update the effectiveness values for the new countermeasure. If you select Quit, the security plan formulation will not accurately reflect the strengths and weaknesses of your IS security posture. SPAN also will be unable to accurately recommend a set of countermeasures.

Following data integrity check, you will be presented with the **Plan** menu. (Figure A-30) This menu allows you to choose the method in which to format your draft security plan.

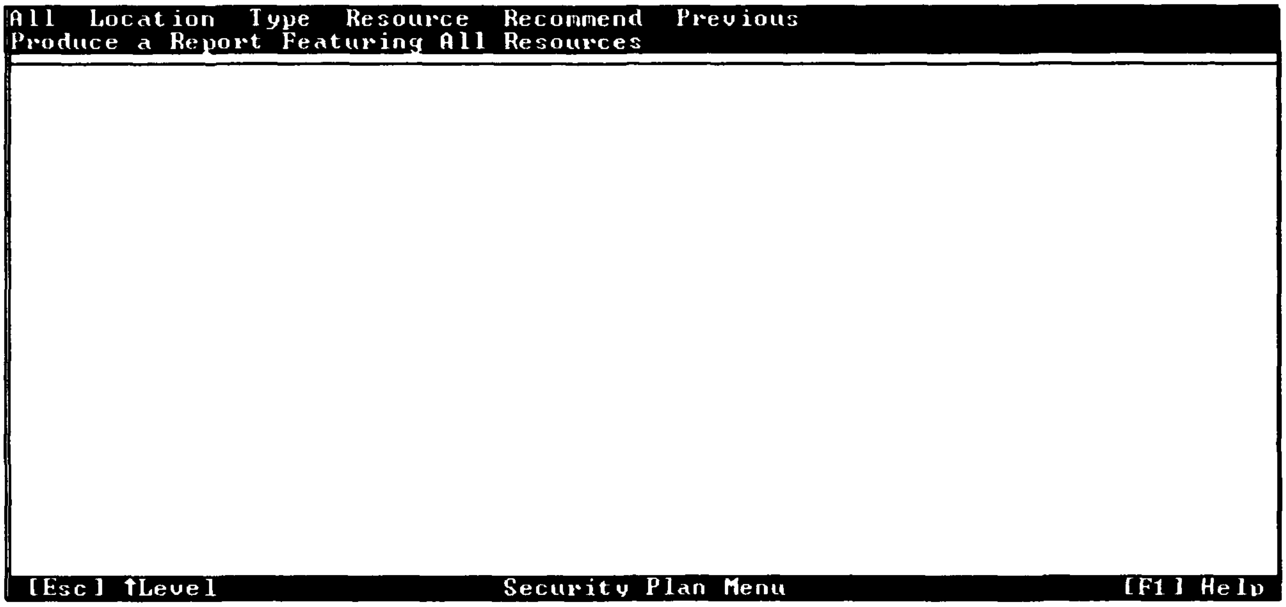

All Location Type Resource Recommend Previous
Produce a Report Featuring All Resources
[Esc] ↑Level
Security Plan Menu
[F1] Help

Figure A-30 Plan Menu

(1) All. The All selection generates a draft security plan featuring all locations and resources in the organization. This is the core of all of SPAN's reports. The plan may be sent to the printer or screen.

(2) Location. The next three selections create reports that are subsets of the ***All*** report. The Location selection will allow you to enter the name of a specific location in the organization. The resulting draft security plan will feature the designated location and all resources in that location.

(3) Type. This selection generates draft security plans that list only resources of a designated type.

(4) Resource. The Resource selection allows you to create a draft security plan that highlights a single resource and the threats and countermeasures that apply to it.

(5) Recommend. This final selection allows SPAN to create its own version of a draft security plan. SPAN will select countermeasures from its database that have not been implemented and can be of practicable use to the organization. Security

plans displaying recommended countermeasures may be generated in each of the four formats previously mentioned.

6. Sensitivity Menu

The Sensitivity selection allows you to perform analysis through "what if" scenarios. SPAN provides this function by creating a set of data identical with the one residing in the database. The data conversion process may take a minute or more to complete. You should be aware that this procedure begins immediately after selecting Sensitivity.

The menu choices available in Sensitivity option are identical with those found in the main menu. The structure and format of the **Sensitivity** menu are found in Figures A-31 and A-32.

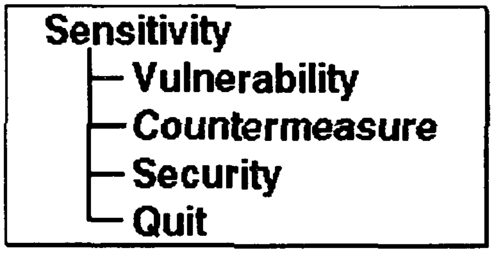
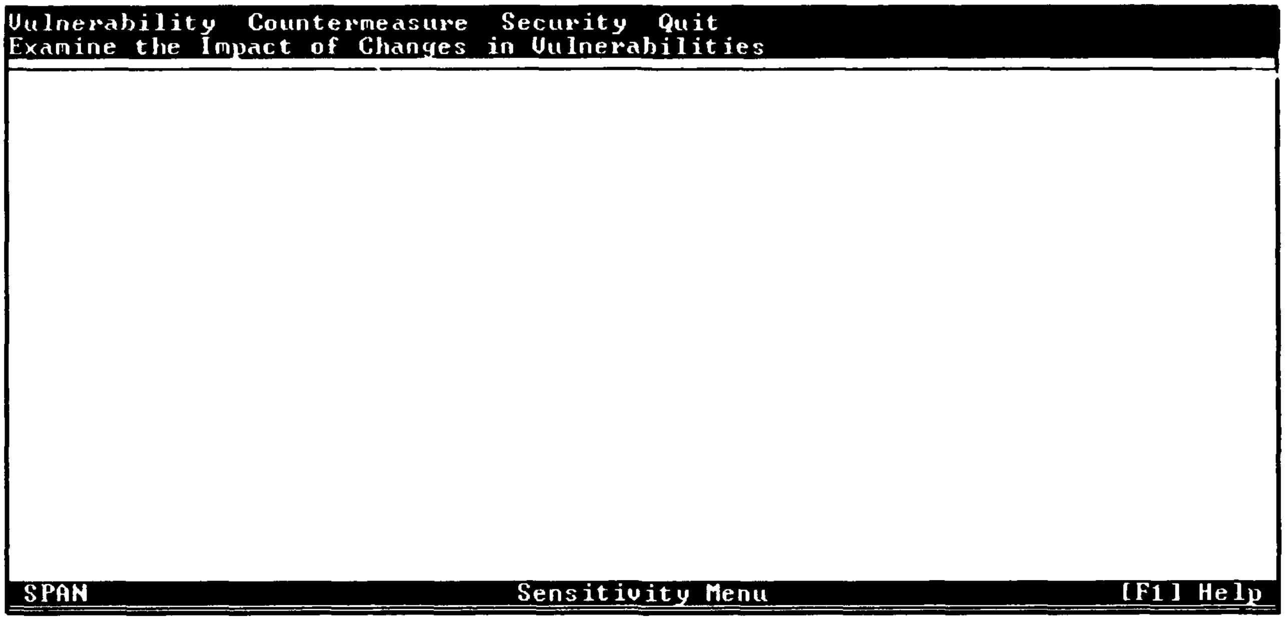


Figure A-31 Sensitivity Menu Structure



Examine the Impact of Changes in Vulnerabilities

Figure A-32 Sensitivity Menu

a. ***Vulnerability***

The Vulnerability selection allows you to modify, add or delete potential threats. You also may change the assignment of threats. The full set of vulnerability reports are available and reflect the change caused by your modifications.

b. ***Countermeasure***

This selection allows you to change modify, add or delete countermeasures. Countermeasures can be implemented or removed from locations and resources. You may view the results of your changes by using the countermeasure reports.

c. ***Security***

The Security selection provides the best perspective of the sensitivity analysis procedure. The draft security plans combine new threat and countermeasure information and show the relationships between them.

d. Quit

This selection will exit **Sensitivity** and return to the **Main** menu. SPAN will execute a data restoration procedure that may take a minute or more to conclude.

APPENDIX B

CASE STUDY - SPAN IN ACTION

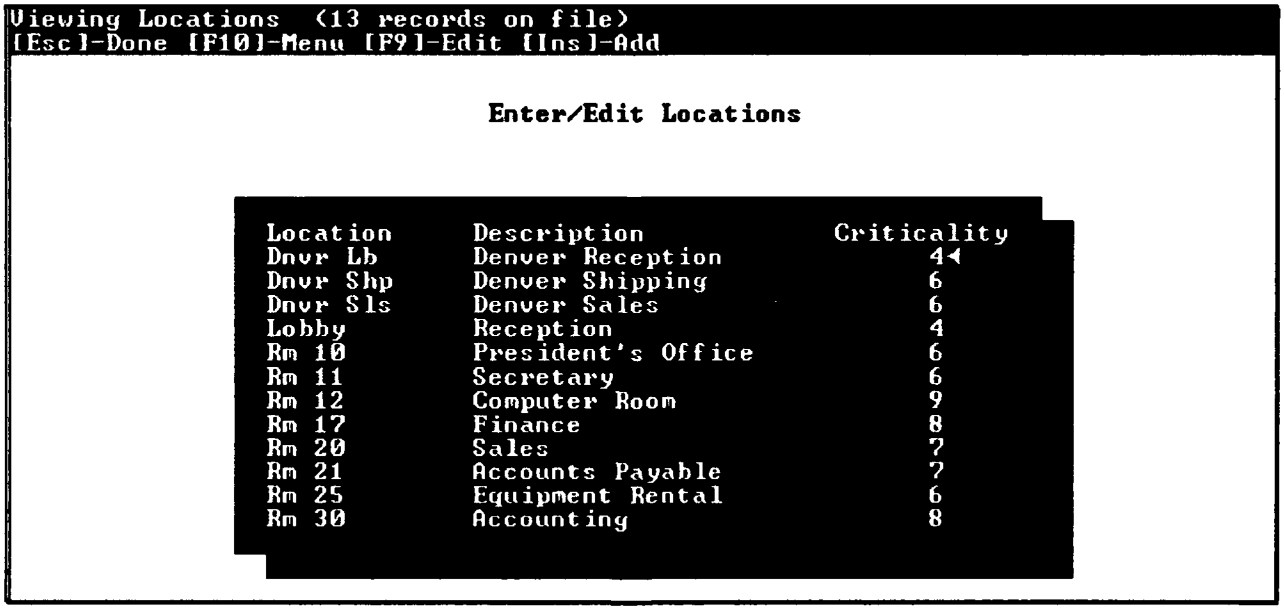
SPAN was implemented and tested in a medium size distributor of products used by the broadcast industry. Their product line included video tape, cameras and editing equipment. They also sold and leased microwave telecommunications equipment. The company had experienced rapid growth, doubling its sales in just one year. Its work force grew to 53 employees, up from 25 employees one year prior. The company's headquarters were located in the southwestern United States with 12 regional offices located throughout the country. The tests were conducted during the spring of 1991.

The computing facilities of the organization were physically centralized in a single room in the company's headquarters. They consisted of a network server, a minicomputer and an array of peripherals. These included a gat^eway, a rack of eight high speed modems, two dot matrix printers and two laser printers. All original copies of software and documentation were stored in the central computer room. The local area network contained 15 PC workstations located in offices within the corporate headquarters. Each regional office had a PC, modem, dot matrix and laser printer.

Before SPAN's implementation, this firm had not planned for its IS security. The only security afforded to its IS resources were the normal security measures taken for the headquarters and offices. Each office had a sprinkler and alarm systems that were installed to protect their inventories. The company was at a period in its growth and development when it became dependent on its IS resources for its survival. It had become evident to management that it was time take another look at IS security.

SPAN was implemented and used at the company's headquarters. It was installed as a single user application on a microcomputer belonging to the finance manager. The finance manager was appointed IS security manager and charged with the responsibility of developing the company's IS security plan.

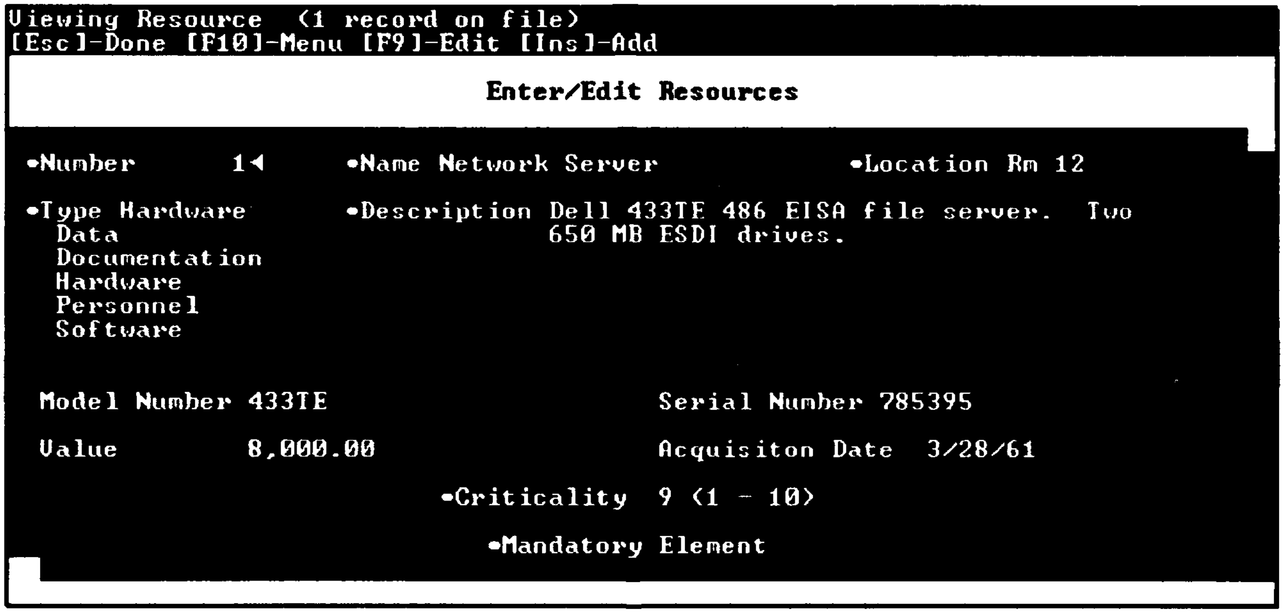
After a brief training session, the newly appointed IS security manager began his first SPAN session. The most time consuming portion of the SPAN process is the entering of resources. Each location that contains IS resources was entered into SPAN. (Figure B-1) This included the central computer room at the corporate headquarters and each office in the headquarters that contained an IS resource. The regional offices were also entered into SPAN's database. Only rooms that contained IS resources were entered. Each regional office had an average of six rooms, three containing IS resources. When the location entries were completed, it was found that the company had IS resources in 49 separate locations housed in 13 sites across the United States.



```
Viewing Locations  (13 records on file)
[Esc]-Done [F10]-Menu [F9]-Edit [Ins]-Add

                       Enter/Edit Locations

        Location      Description              Criticality
        Dnvr Lb       Denver Reception              4◄
        Dnvr Shp      Denver Shipping               6
        Dnvr Sls      Denver Sales                  6
        Lobby         Reception                     4
        Rm 10         President's Office            6
        Rm 11         Secretary                     6
        Rm 12         Computer Room                 9
        Rm 17         Finance                       8
        Rm 20         Sales                         7
        Rm 21         Accounts Payable              7
        Rm 25         Equipment Rental              6
        Rm 30         Accounting                    8
```

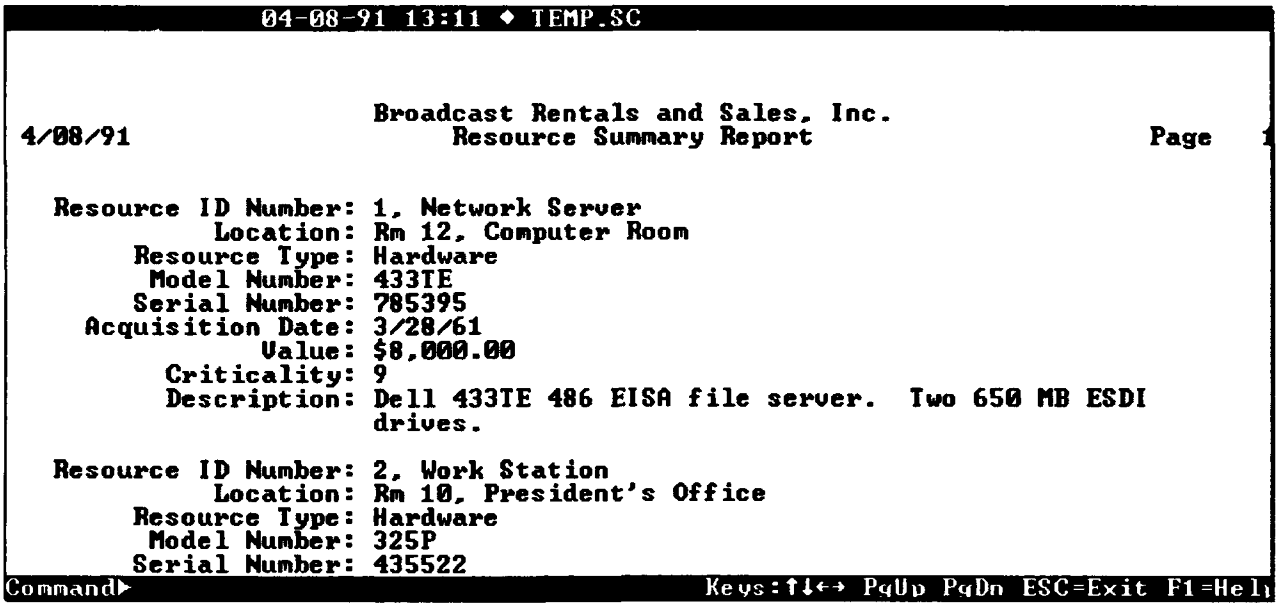
Figure B-1 Location Form

The next step involved entering individual resources. (Figure B-2) The hardware consisted of the items listed above. Also included in the database were all original copies of the software owned and used by the company, software and hardware documentation and off-line and backup storage media. The number of records added to the database was well beyond the expectations of the security manager. This was the first time that anyone in the company had created an inventory of their IS resources. SPAN's summary report gave the manager an itemized list of resources sorted by location. (Figure B-3)



```
Viewing Resource  (1 record on file)
[Esc]-Done [F10]-Menu [F9]-Edit [Ins]-Add

                             Enter/Edit Resources

•Number       1◄     •Name Network Server            •Location Rm 12

•Type Hardware       •Description Dell 433TE 486 EISA file server.  Two
  Data                            650 MB ESDI drives.
  Documentation
  Hardware
  Personnel
  Software

 Model Number 433TE                     Serial Number 785395

 Value        8,000.00                  Acquisiton Date  3/28/61

                        •Criticality  9 (1 - 10)

                           •Mandatory Element
```

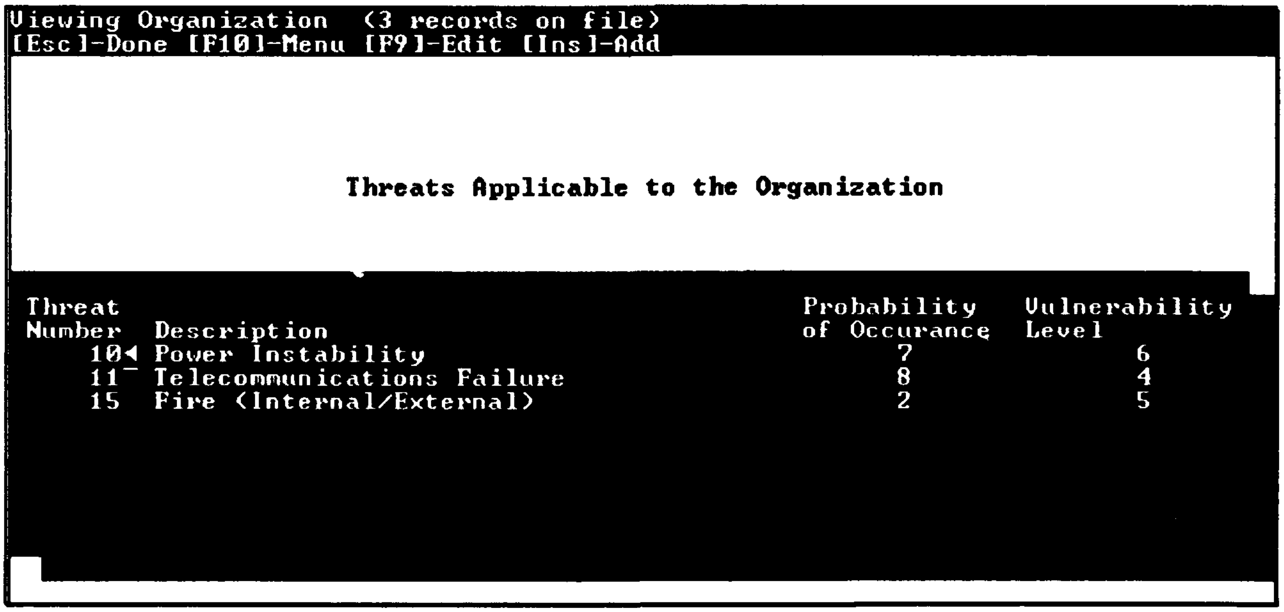
Figure B-2 Resource Form



```
                        04-08-91 13:11 ◆ TEMP.SC


                                Broadcast Rentals and Sales, Inc.
 4/08/91                             Resource Summary Report                         Page 1

   Resource ID Number: 1, Network Server
             Location: Rm 12, Computer Room
        Resource Type: Hardware
         Model Number: 433TE
        Serial Number: 785395
     Acquisition Date: 3/28/61
                Value: $8,000.00
          Criticality: 9
          Description: Dell 433TE 486 EISA file server.  Two 650 MB ESDI
                       drives.

   Resource ID Number: 2, Work Station
             Location: Rm 10, President's Office
        Resource Type: Hardware
         Model Number: 325P
        Serial Number: 435522
Command▶                                            Keys:↑↓←→ PgUp PgDn ESC=Exit F1=Hel
```

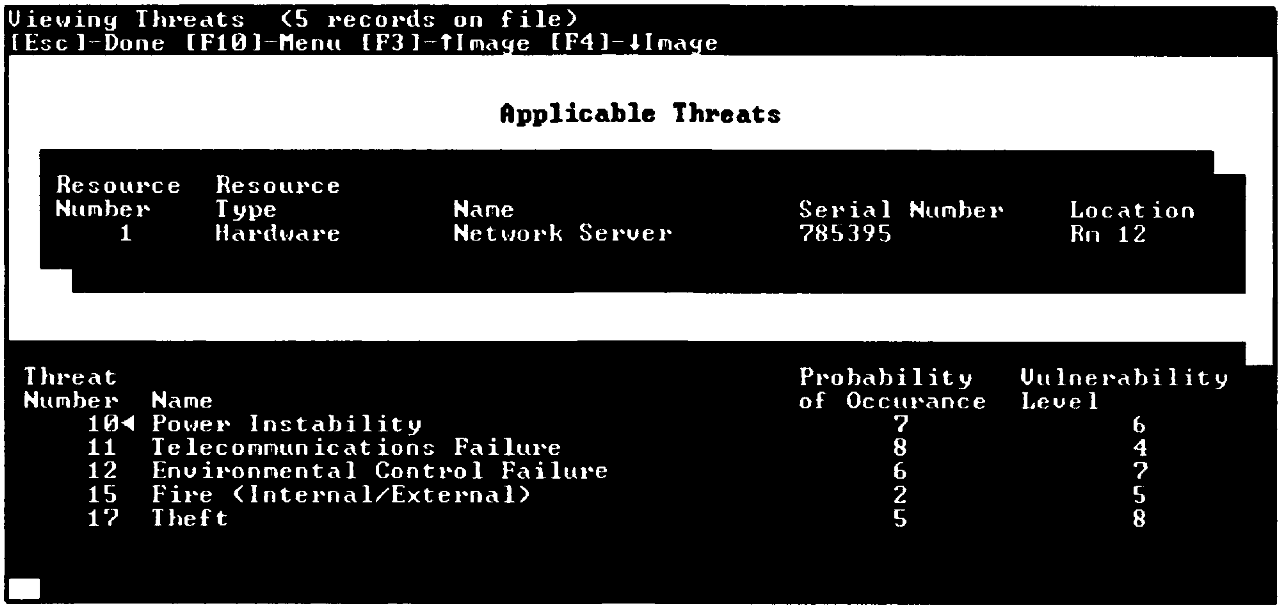
Figure B-3 Summary Report

After the completion of the location and resource entries, applicable threats were identified and assigned and vulnerabilities were evaluated. SPAN's initial database of threats contained all of the threats that were found applicable to the organization. Existing countermeasures were then applied to threats.



```
Viewing Organization  (3 records on file)
[Esc]-Done [F10]-Menu [F9]-Edit [Ins]-Add


                        Threats Applicable to the Organization


 Threat                                              Probability   Vulnerability
 Number  Description                                 of Occurance  Level
    10◀  Power Instability                                7              6
    11¯  Telecommunications Failure                       8              4
    15   Fire (Internal/External)                         2              5
```

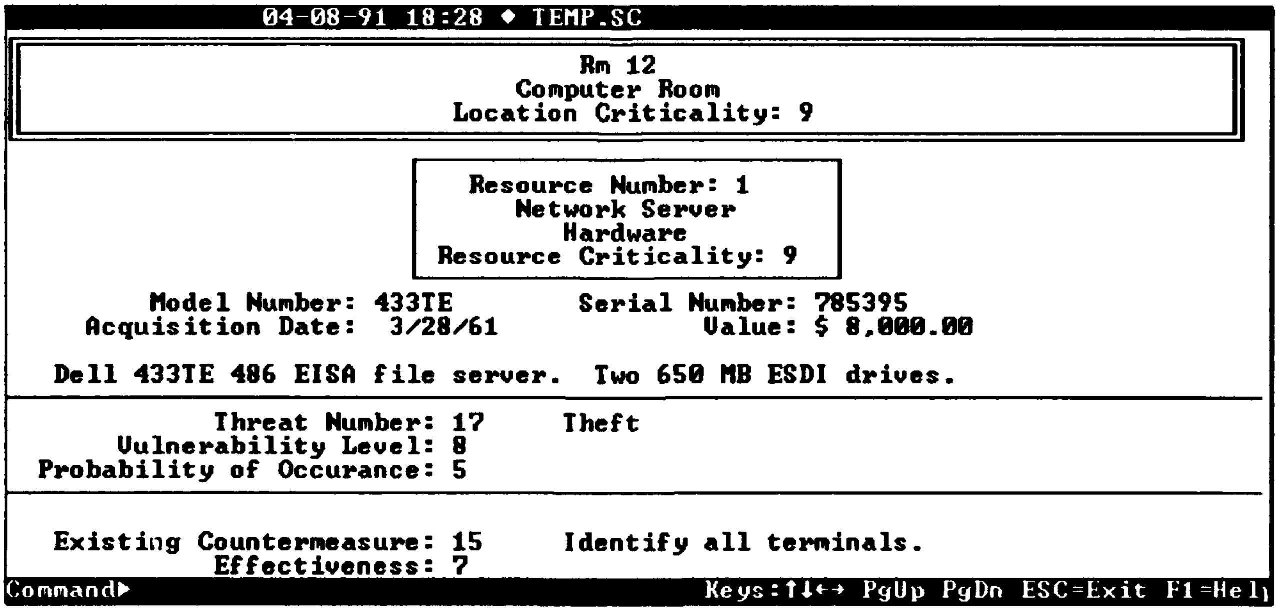
Figure B-4 Threats Applicable to the Organization



```
Viewing Threats  (5 records on file)
[Esc]-Done [F10]-Menu [F3]-↑Image [F4]-↓Image

                         Applicable Threats

 Resource  Resource
 Number    Type        Name                 Serial Number   Location
    1      Hardware    Network Server       785395          Rm 12

Threat                                     Probability  Vulnerability
Number  Name                               of Occurance Level
   10◄  Power Instability                      7             6
   11   Telecommunications Failure             8             4
   12   Environmental Control Failure          6             7
   15   Fire (Internal/External)               2             5
   17   Theft                                  5             8
```

Figure B-5 All Threats Assigned

SPAN created a draft security plan based on the existing threats and countermeasures. (Figure B-6) The plan was reviewed by senior management, who then ran several iterations of SPAN's sensitivity analysis function. Each iteration contained a different mix of proposed countermeasures and added additional probable threats.



```
                 04-08-91 18:28 ◆ TEMP.SC
                          Rm 12
                      Computer Room
                  Location Criticality: 9

                    Resource Number: 1
                      Network Server
                         Hardware
                  Resource Criticality: 9

     Model Number: 433TE        Serial Number: 785395
 Acquisition Date:  3/28/61             Value: $ 8,000.00

   Dell 433TE 486 EISA file server.  Two 650 MB ESDI drives.

          Threat Number: 17     Theft
     Vulnerability Level: 8
 Probability of Occurance: 5

   Existing Countermeasure: 15     Identify all terminals.
             Effectiveness: 7
Command▶                       Keys:↑↓←→ PgUp PgDn ESC=Exit F1=Hel
```

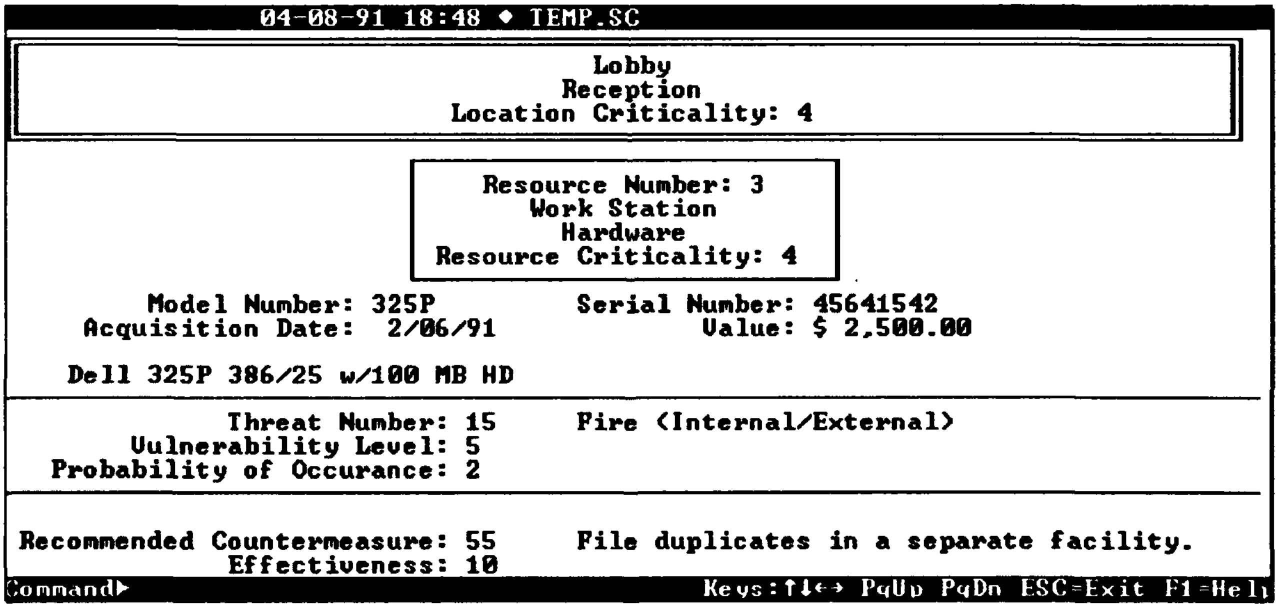
Figure B-6 Draft Security Plan

SPAN recommended the organization add a full set of countermeasures. (Figure B-7) This analysis was based on the user defined location and resource entries and SPAN's default set of threats and countermeasures. The following is a subset of the list of recommended countermeasures.

1. Use keywords or passwords whenever possible.
2. Place tapes in their containers when not being used.
3. Keep a log of all personnel who have had access to sensitive data banks.
4. Record and classify all programs.
5. Conduct checks to ensure accuracy of the backup system.
6. File duplicates in a separate facility.
7. Limit valid users access to specific files.

8 Locate library in a secure area.

9. Conduct periodic spot checks to detect and minimize misuse or abuse of the system.



```
                    04-08-91 18:48 ◆ TEMP.SC

                              Lobby
                            Reception
                     Location Criticality: 4

                       Resource Number: 3
                          Work Station
                            Hardware
                     Resource Criticality: 4

        Model Number: 325P          Serial Number: 45641542
     Acquisition Date:  2/06/91             Value: $ 2,500.00

   Dell 325P 386/25 w/100 MB HD

               Threat Number: 15    Fire (Internal/External)
         Vulnerability Level: 5
    Probability of Occurance: 2

Recommended Countermeasure: 55      File duplicates in a separate facility.
             Effectiveness: 10
Command▶                            Keys:↑↓←→ PgUp PgDn ESC=Exit F1=Hel
```

Figure B-7 Recommended Countermeasures

After reviewing the feasibility of implementing the recommended countermeasures and their effect on the company and its computing facilities, management adopted these recommendations as part of the organization new IS security plan.

SPAN made the security plan analysis procedure more efficient and adaptable. The flexibility afforded by SPAN will allow this company to modify their IS security plan to account for unexpected changes in conditions without starting the process over. Without the software, security plan analysis can be a long and tedious process.

LIST OF REFERENCES

Alexander, M. "Users Get Serious About Growing Security Risk." Computerworld 5 August 1991: 1.

Awad, E.M. Management Information Systems: Concepts, Structure and Applications. Menlo Park: Benjamin Cummings, 1988.

Bequai, A., How to Prevent Computer Crime. New York: John Wiley & Sons, 1983.

Bidgoli, H. and Azarmsa, R. "Computer Security: New Managerial Concern for the 1980's and Beyond." Journal of Systems Management 40.10 (1989): 21.

Bodily, S. E. Modern Decision Making. New York: McGraw-Hill, 1985.

Brown, W. F., ed. Computer and Software Security. New York: AMR International, 1971.

Browne, P. S. Security: Checklist for Computer Center Self-Audits. Arlington: American Federation of Information Processing Societies, 1979.

Carroll, J. M. Computer Security. 2nd ed. Boston: Butterworths, 1987.

Datapro. "Risk Analysis Software." Datapro Reports on Information Security 6.8 (1990): 151-153.

Diehl, S., Wszola, S., Kliewer, B. and Stevens, L. "Prescription for Safer Data." BYTE, August 1991: 218-235.

Hsiao, D. K., Kerr, D. S. and Madnik, S. E. Computer Security. New York: Academic Press, 1979.

Jackson, C. B. "The Need for Security." Datapro Reports on Information Security 6.10 (1990): 101-134.

Kalman, D. and Poor, A. "15 Relational Databases: Easy Access, Programming Power." PC Magazine 28 May 1991: 101-200.

Kelly, M. "The Risk Business." Practical Computing 11.12 (1988):91.

Lane, V. P. Security of Computer Based Information Systems. Houndmills: Macmillan Education Ltd., 1985.

Palmer, I.C. and Potter, G. A. Computer Security Risk Management. New York: Van Nostrand Reinhold, 1989.

Pfleeger, C. P. Security in Computing. Englewood Cliffs: Prentice Hall, 1989.

Powell, K. "Software Program Defines SBA's Security Needs." Government Security News 7.24 (1988): 97-98.

Ruthberg, Z. G., ed., and McKenzie, R. G., ed. Audit and Evaluation of Computer Security. Washington: U.S. Government Printing Office, 1977.

Sprague, R. H. and Carlson, E. D. Building Effective Decision Support Systems. Englewood Cliffs: Prentice-Hall, 1982.

Sprague, R. H. and Watson, H. J., ed. Decision Support Systems: Putting Theory Into Practice. 2nd ed. Englewood Cliffs: Prentice-Hall, 1989.

Tomkins, F.G. "How to Select a Risk Analysis Software Package." Datapro Reports on Information Security 7.3 (1989): 101-107.

Turban, E. Decision Support and Expert Systems. 2nd ed. New York: Macmillan, 1990.

Van Zanten, A., Coumou, C. and Schouten, T. "Computer Aided Security: An Expert System for Managing Risk." 2nd European Conference on Computer Audit, Control and Security. Amsterdam: Dutch Assoc. Inf., 1987.

Walker, B. J. and Walker, I. F. Computer Security and Protection Structures. Stroudsburg: Dowden, Hutchinson & Ross, Inc., 1977.

Zenreich, A. and Kocis, J. M. Paradox Programmers Guide: PAL by Example. Scott Foresman, 1990.

Zviran, M., Hoge, J. C. and Micucci, V. A.. "SPAN - A DSS for Security Plan Analysis." Computers & Security 9 (1990): 153-160.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
Cameron Station
Alexandria, Virginia 22304-6145

2. Library, Code 52 2
Naval Postgraduate School
Monterey, California 93943-5002

3. Professor Moshe Zviran 1
Department of Administrative Sciences
Code AS/Zv
Naval Postgraduate School
Monterey, California 93943

4. Professor William Haga 1
Department of Administrative Sciences
Code AS/Hg
Naval Postgraduate School
Monterey, California 93943

5. Lieutenant Stephen H. Ramsey 1
4237 W. Ponds Circle
Littleton, Colorado 80123