This is to certify that the

dissertation entitled

A PROGRAM EVALUATION OF SAMARITAN HEALTH CENTER'S DEPARTMENT OF PROTECTIVE SERVICES:

A NEW MODEL FOR PROVIDING PROTECTION IN HEALTH CARE ENVIRONMENTS

presented by

Robert Allen Smith

has been accepted towards fulfillment
of the requirements for

Ph.D. degree in Social Science

Kenneth E. Christian
Major professor

Date June 21, 1989

A PROGRAM EVALUATION OF SAMARITAN HEALTH CENTER'S DEPARTMENT OF PROTECTIVE SERVICES:

A NEW MODEL FOR PROVIDING PROTECTION IN HEALTH CARE ENVIRONMENTS

By

Robert Allen Smith

A DISSERTATION

Volume I

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

School of Criminal Justice

1989

ABSTRACT

A PROGRAM EVALUATION OF SAMARITAN HEALTH CENTER'S DEPARTMENT OF PROTECTIVE SERVICES:

A NEW MODEL FOR PROVIDING PROTECTION IN HEALTH CARE ENVIRONMENTS

By

Robert Allen Smith

The purpose of this study is twofold. First, it represents a straightforward evaluation of a reorganized security program at an inner-city hospital. Second, it also constitutes a field test of a theoretical model, which was created for the overall management of security programs in general, and upon which the reorganized security program was itself developed.

Programmatic goals and objectives were employed as the functional equivalents of formal hypotheses. There were a total of 20 goals and 127 corresponding objectives, covering all aspects of the reorganized security program. Most of the data relating to these goals and objectives took the form of crime, security and service related statistics, as well as employee attitudinal measures toward the program.

A pretest-posttest-posttest research design was primarily employed to allow comparisons of the year before the security program's reorganization and the two years following it. Analysis was accomplished in two different

ways. Certain nonquantitative objectives were evaluated by a panel of hospital administrators. For the quantitative objectives frequency tables, distributions and percentages were calculated and compared. Two-Tailed T-Tests of the differences in means were also conducted for some variables.

One-hundred twenty three of the 127 objectives were met and all 20 goals were achieved. (This equated to the acceptance of all hypotheses in a more conventional study.) In the first posttest year, crimes and security-related incidents decreased in all categories from the pretest year. A greater variety and number of miscellaneous services were provided. The self-perceptions of the security personnel improved significantly. The perceptions of the employee sample toward the security program also improved significantly.

The findings for the second posttest year were equal to, and in many cases even better than, those for the first posttest year. As a result, it is reasonable to conclude that the reorganized security program itself was highly successful. It can also be safely inferred that the theoretical model, upon which it was developed and conducted, had considerable utility as a management tool.

This study is dedicated to the two most important women in my life, Dr. Karen Larson who was my wife and friend for eight years, and Meagan Ashleigh Smith who will be my daughter and friend forever.

ACKNOWLEDGMENTS

This study could have never been completed without the unselfish contributions of a large number of people. It is only fitting that they receive some degree of recognition here, because they certainly deserve it.

The first "unsung hero" is Mary Jo Mercer. Not only did she do a masterful job of typing this document, but she was also able to decipher my handwriting, which is no easy task for even a cryptographer.

The members of my dissertation committee, Professors Gerald Miller, John Hunter, and Robert Trojanowicz, all deserve credit and thanks for sharing their time, expertise and patience. To even have this elite group of academicians on my committee was an honor.

A very special note of thanks is due to Professor Kenneth Christian, who chaired my committee. To say that Ken was a driving force in completing the study would be an understatement. His guidance and support were invaluable. I would never have finished without him.

Finally, an immeasurable amount of credit goes to the members of the Department of Protective Services at Samaritan Health Center, who actually achieved the results described in this document. I've never served with a finer group of people.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

NEED

The nation's healthcare institutions are generally viewed as "havens" within which the sick and injured can receive professional care in a safe, secure, and controlled environment. There is an implicit assumption that hospitals are "special" places, immune to many of the problems of the "real" world, such as crime. Unfortunately, nothing could be further from the truth.

A hospital is the functional equivalent of a vertical city and, as such, faces the same problems as other municipalities. In fact, a hospital's potential vulnerability actually exceeds that of its surrounding community. The typical hospital has all the "high risk" targets usually associated with most street crimes. These include cars, drugs, high-tech equipment, cash, retail services and merchandise, personal valuables, helpless victims (i.e., patients), and a large ratio of female employees working all shifts. In addition, disturbed, disoriented, distraught, overdosed, or intoxicated persons often vent their emotions, anxieties, anger, and frustrations in hospitals. Furthermore, many crime related problems, which actually originate

in surrounding neighborhoods, often end up at the nearest hospital, especially in the emergency room, lobby, patient units, or parking lots.

In spite of the potential risks, the general protective response has been historically minimal. Seldom do hospitals receive the same level of police protection as their surrounding neighborhoods. Police respond to problems "after the fact," if they are available, but they do not routinely patrol the healthcare environments. That job is relegated, if at all, to a security force, either proprietary or contract, which has traditionally lacked the resources, training, professionalism, and administrative support to adequately control its own environment. In effect, hospital security is more often an afterthought, rather than a preconceived priority, and security personnel are commonly considered as necessary "evils," who do not contribute to patient care, nor generate revenue for the institution.

The healthcare security field, as a profession, is still in its infancy and suffers from the negative stereotype associated with unqualified "guards." While significant steps have been made in recent years to improve on this image, there is still widespread ignorance and benign neglect on the part of healthcare decisionmakers. This, in turn, has perpetuated a limited ability to protect our healthcare facilities.

A classic example of the problems faced by healthcare security departments, can be found at Samaritan Health Center, a 375-bed acute care community hospital in inner-city Detroit. It is a Catholic institution, with a mission to serve the poor and indigent. It was "born" from a merger of two older hospitals in 1980.

In 1982, construction was begun on a new replacement facility, which would consolidate both older hospitals. The proposed location of this replacement facility caused considerable concern on the part of the employee population, because it was in virtually the highest crime neighborhood of the city. This was in contrast to the relatively low crime areas where the older hospitals had been located. (One was under the shadow of Detroit Police Headquarters and the other was in a well-patrolled area on a main thoroughfare.) In fact, the immediate neighborhood surrounding the new site, which was routinely patrolled by only one police vehicle, had experienced a steady increase in crime over time, culminating in 1983 with six homicides and approximately 100 robberies, 20 rapes, 200 vehicle thefts, 100 assaults, and 200 burglaries (all within a half-mile or less of the new facility).[1] The prospect for the future was not promising either. The city was in the process of regaining the dubious distinction of being the "murder capital of the world," and recent police lay-offs had decimated the department by approximately 25 percent, with no reversal of the trend in sight at that time.

Employee perceptions reflected the actual crime statistics. Sixty-two percent of the employee population indicated a belief that crime problems would increase with the move to the new site.[2] Ninety-three percent felt that an effective security program was vital to the actual survival of the new hospital.[3] In fact, personal safety and security was widely accepted as being the single greatest concern associated with the impending move.[4]

Moreover, employee concern was further heightened because of a general lack of confidence in the existing security department. It was widely viewed as already being ineffective at the older hospitals and, therefore, incapable of effectively dealing with the anticipated increase in crime problems at the new site.

To compound these dilemmas, a legal issue of great concern arose. According to Michigan State law, a private citizen such as a hospital security guard is only authorized to make an arrest:

1) for a felony committed in his presence,

2) when the person to be arrested has committed a felony although not in his presence, or

3) when summoned by any peace officer to assist said officer in making an arrest.[5]

Specifically omitted is the legal authority to arrest for a misdemeanor, which is granted to fully sworn peace officers.[6] Also denied to private citizens is what has been commonly called "probable cause protection." The statute, giving peace officers their arrest authority, also makes

provision for felony arrests based on probable cause. This, in effect, provides peace officers with a legal defense, both criminally and civilly, against charges of false arrest, when the test for probable cause has been met. This "test" is ultimately a court decision on whether or not the arresting officer had sufficient reason to believe that a crime had been committed and that the person arrested was the perpetrator. However, this does not apply to private citizens who are much more vulnerable to criminal and/or civil charges of false arrest, false imprisonment, abduction or even assault-and-battery, if they make an honest error in their arrest or if, for some other reason, a conviction is not subsequently obtained.

At the surface, this lack of legal authority to make misdemeanor arrests or enjoy probable cause protection should not seem to be very problematic, because private security guards seldom deliberately place anyone under arrest. Unfortunately, most crimes committed in a hospital are in fact misdemeanors, such as trespassing, disorderly conduct, simple larceny, or assault-and-battery. Detaining such offenders (even if only until the police arrive) technically constitutes an arrest which has been defined as . . . "the subjecting of a person to physical control or its equivalent (i.e., indication oF immediate ability to control physically)."[7]

Even the act of handcuffing a violent person for everyone else's protection is technically an arrest, whether

or not the person is so informed. Moving the person to a secluded area can be considered abduction. Keeping him in a holding area until the police arrive can be false imprisonment. The very act of physically overpowering an assailant can be argued to be assault-and-battery itself, especially if he stops fighting or resisting during the process. To make matters worse, a security guard's employer is also exposed to legal action under the general principle of Vicarious Liability.

While these examples may seem absurd, they are in fact legitimate realities. They place most private security personnel in a "Catch 22" situation. Officers are legally (and morally) obligated to protect their environment, but not legally authorized to do so in many cases.

Historically, this "no win" situation was not much of a practical problem. Most citizens were simply not aware of the legal constraints involved and recourses available, so litigation was rare. However, at about the time that Samaritan Health Center's replacement facility was being constructed, this changed. In Wayne County, which has a reputation for large dockets of civil suits and higher-than-average monetary awards, several false arrest suits were being initiated.[8] Each of them involved misdemeanor offenders in hospital environments who were overpowered or detained by security personnel until the Detroit Police arrived. Some of them had even received mass media attention. The Detroit Police Department then became

concerned about its own potential liability in receiving these misdemeanor "prisoners" from hospital security guards. A memo was issued from the chief to all precinct commanders in late 1982 putting an end to this practice. In effect, the thin ice, upon which private security guards had been treading for years, was crumbling.

Samaritan Health Center now had three distinct problems. It was moving into a high crime area, had a security force with the reputation of being the worst department in the hospital, and lacked the legal authority to take action against some of its anticipated problems. Furthermore, the Police Precinct Commander at the replacement facility's location could not promise increased police coverage to protect the hospital once the move was made. Many hospital employees even threatened to quit if they were not guaranteed better protection at the new site.

In order to resolve these problems, the Administration and Board of Directors at Samaritan Health Center were willing to take drastic steps and consider all options available. They simply had to have a better security force which could protect the institution without incurring unnecessary liability.

While possibly more acute than many other institutions, Samaritan Health Center's dilemma was by no means unique. All hospital security departments in the State (and many other states for that matter) were in the same legal situation. Hence any solutions, which might be developed at

Samaritan, could easily be applicable to the rest of the field. On the one hand, Samaritan was faced with a potentially serious set of problems. On the other hand, these problems themselves presented a rare opportunity for advancing the state-of-the-art in the healthcare security field and developing a prototype or model program which could significantly contribute to the industry's needs.

PURPOSE

The purpose of this study can be examined at two levels of analysis. At the most basic level, it is a straight-forward program evaluation of the security reorganization at Samaritan Health Center. In a broader sense, however, it also represents a case study of the implementation of a new and innovative model for managing healthcare security programs in general.

Given this dual focus, the study can be described in organizational development (O.D.) terminology as an example of Action Research, which is defined as:

> . . . the systematic attempt . . . to bring about change in an organization and at the same time, to generate new scientific knowledge which can be replicated, verified, and added to our knowledge of behavioral science.[9]

HYPOTHESES

The driving force for reorganizing the security program at Samaritan Health Center (S.H.C.) was the concern to provide a safe and secure environment for patients, staff,

and visitors. This "reason-to-be" was translated into the following mission statement:

> The mission of the Department of Protective Services is to protect and service the hospital, its patients, visitors, employees, and medical staff. This shall be accomplished through the systemic and cost-effective integration of technology, personnel, and prevention/control programs.

In the course of satisfying this somewhat broad and general mandate, a number of related programmatic goals had to be established and attained. They formed the basis for the hypothesis of this study and are listed below in a somewhat different format as general research questions:

1) Can the reorganized program prevent the occurrence of security . . . related incidents which may result in personal harm, property loss, legal liability, and disruption of routine hospital operations?

2) Can the reorganized program minimize the degree of harm, loss, liability, and disruption associated with those incidents which cannot be prevented?

3) Can the reorganized program correct and/or eliminate the underlying problems which either cause or allow incidents to initially occur?

4) Can the reorganized program provide those miscellaneous services required for the general welfare and efficient operations?

5) Can the reorganized program's resources be effectively acquired, developed, and maintained?

6) Can the reorganized program's resources be effectively utilized and managed?

7) Can fiscal constraints be adhered to in a cost-efficient manner?

8) Can a healthy organizational climate be maintained which fosters positive working relationships and teamwork?

9) Can the reorganized program convey a positive image within the health center and community which promotes confidence, trust, cooperation, and favorable public relations?

10) Can effective communication links be maintained within the department, health center, and community?

These research questions, when rephrased as statements, form the basis for the strategic and supportive goals upon which the reorganized program focused. They also constitute the functional equivalent of formal hypotheses. While presented here in somewhat abstract form, they will be reintroduced in more concrete, operational terms in Chapter 4 as a series of primarily quantifiable objectives for each goal statement. It will be these individual objectives which are tested. In order to a particular research question to be answered in the affirmative, its corresponding objectives must be achieved.

THEORY

The initial driving force for reorganizing S.H.C.'s security program was to correct an immediate problem, not to build nor test any specific, formal theory related to crime prevention and control. However, the effort was formulated, executed and evaluated within the parameters of a theoretical model which the author had previously constructed for just such a purpose. More specifically, in 1982, before assuming responsibility for the security

program at S.H.C., the author was approached and contracted by the Michigan Hospital Association to develop guidelines for managing hospital security programs. The mandate was to develop a training manual for hospital security managers which would:

1) be comprehensive enough to address all major duties and responsibilities associated with managing security departments,

2) provide effective methodologies for planning, executing, and evaluating security programs,

3) incorporate state-of-the-art technologies, prevailing management philosophies and techniques, sound academic principles related to the field, and practical experience-based insights into those procedures, and

4) present this body of knowledge in a format and at a level of comprehension that the average practitioner could understand, assimilate and apply on a daily basis.

In effect, what was required was a "primer" on hospital security management, that bridged the gap between scholarly theory and real world reality. The result was a comprehensive and lengthy document organized around a generic planning model. The ACTION MODEL was comprised of a broad cross-section of perspectives and principles of program development in general and security management in particular. While it will be described in full detail in Chapter 3, its major tenets can be summarized, as follows:

1) A successful security program is based on three continuous, and cyclical activities, planning, execution, and evaluation.

2) A successful security program is goal-directed with congruent and measurable results or objectives that drive all operations and activities.

3) Goals and objectives must be translated into operational plans which are carried out, evaluated, and modified, as necessary.

4) An effective security program must be organized, understood, and managed within the context of a general systems theory. More specifically, it is a vital subsystem of a larger healthcare system. It has three major components: people, property, and practices, which can be examined, understood, and applied at several different levels of analysis (i.e., system levels.)

5) Effective decision-making and problem-solving require a certain pattern of cognitive steps which are integrally intertwined with all other activities described above.

OVERVIEW

Due to the somewhat unique nature and focus of this study, it has been organized and formatted in somewhat different fashion than is traditional for most doctoral dissertations. More specifically, it has been organized into the following chapters:

Introduction

Review of the Literature

Theoretical Framework

Design and Methodology

Implementing the Program

Data Analysis

Summary and Conclusions

In Chapter 2, a brief discussion on the current status of scholarly literature in the field will be provided. As the reader will discover, no directly comparable research effort has yet been published. In fact, little research has been conducted at all.

In Chapter 3, the ACTION MODEL will be described in terms of its major processes, related tasks, and functional components. Also addressed will be several supplemental stratagems (or conceptual models in their own right) which can be applied with the ACTION MODEL itself. These include a simple design-making/problem-solving scheme, a "general systems" view of security programs, a modified management-by-objectives approach and a set of strategies for initiating planned change.

In Chapter 4, the research methodologies, employed in the study, will be described in terms of actual research design, samples, measurement and data collection, concrete hypotheses, and analytical techniques. As the reader will discover, the design and analysis may not be as methodologically sophisticated as would be possible in a more controlled environment. However, they are methodologically sound and will yield reliable and internally valid results, which can be both useful and understandable to "nonacademic" practitioners.

In Chapter 5, the actual steps undertaken in the reorganization of S.H.C.'s security program will be described. This discussion will address all aspects of the

reorganization from initial diagnosis to strategy setting to implementation, all within the context of the theoretical framework outlined in Chapter 3.

In Chapter 6, the actual performance of the program implemented in Chapter 5, will be evaluated. Relevant data will be presented, analyzed, and interpreted, as appropriate. The hypotheses (i.e., goals and objectives) will be tested. Nonquantitative indicators of success will also be examined.

In Chapter 7, the research findings will be summarized and conclusions will be drawn. A discussion on how the study's results relate back to the study's theoretical framework will be presented and the potential implications for future research will also be explored.

FOOTNOTES

[1]Source: Official Detroit Police Department crime statistics in 1983 for the 15th Precinct, Patrol District 4, which surrounds the site of the replacement facility.

[2]Based on the results of a hospital generated survey of administrators, house physicians, department heads, managers, and supervisors (N=105).

[3]See Number 2 above.

[4]Based on a separate survey of all hospital employees, conducted by the Employee Relations Department via mailings. The specific details and respondents were not shared with the author. Instead only the finding that security concerns were the single most reported issue was made available.

[5]Section 764.16 of the Michigan Compiled Laws.

[6]Section 764.15 of the Michigan Compiled Laws.

[7]Handbook of Michigan Criminal Law & Procedures, (Lansing: Mid-Michigan Law Enforcement Center, 1980), pg. 11.

[8]Based on information provided to the author by the Commander of the Private Security and Investigators Section of the Michigan Department of State Police. Five suits resulted in judgments against one Detroit hospital alone for over $10,000 each - Two other suits resulted in awards of $1,300,000 and $1,700,000 at other inner-city hospitals.

[9]Edgar F. Huse, Organization Development and Change (St. Paul, MN.: West Publishing Company, 1980), pg. 28.

CHAPTER 2

REVIEW OF THE LITERATURE

INTRODUCTION

In the review of published security related literature, two glaring observations stand out. First, a considerable amount of lip service has been placed on the need for empirical research in the field. Second, very little action has followed to satisfy that need.

In spite of the fact that " . . . private protection resources in the United States outnumber law enforcement personnel by a ratio of nearly 2:1 . . .,"[10] and that "recent expenditure levels exceeded 21.7 billion dollars as opposed to only 13.8 billion dollars for public police protection"[11] the private security field has been largely devoid of scholarly research, both basic and applied. This represents a massive commitment of human and fiscal resources to a discipline which lacks an empirical research base and a clearly defined, theoretical body of knowledge.

Hundreds of millions of dollars were allocated to the "smaller" public sector in the Sixties and Seventies by the Law Enforcement Assistance Administration of the U.S. Department of Justice for research and development on crime prevention and control. A considerable amount of funds and

effort are still being committed to public sector research today. The lack of similar attention to the private sector is particularly ironic, because as the President's Task Force on Private Security pointed out in 1976:

> The application of the resources, technology, skills, and knowledge of the private security industry presents the best hope available for protecting the citizen that has witnessed his defenses against crime shrink to a level which leaves him virtually unprotected.[12]

THE UNMET NEED

There have only been three significant industry-wide studies conducted to date. Among their other findings and recommendations, all three acknowledge the lack of research in the field and the need to conduct it.

In 1972, the first comprehensive examination of the state-of-the-art in the security industry was published, commonly known as the Rand Report. It noted, " . . . the paucity of existing data and analyses . . ."[13] and proposed the following:

> The federal government should consider funding a research center that would evaluate the effectiveness and costs of private security personnel and equipment.[14]

The report further recommended a dozen specific areas where research would be valuable.

In 1976, the President's Task Force on Private Security took another broad look at the security profession. It made two significant observations regarding the state of research in the field. First, it found that it:

> . . . was entering a field that has not had extensive research and analysis. There are comparative few . . . scholarly treatises concerning the diverse and complex private security field.[15]

Furthermore, it went on to state that

> . . . there has been little emphasis on research as it relates to private security services. The absence of reliable research has made planning and decisionmaking difficult in the field.[16]

Agreeing with the previous recommendations of the Rand Report, the President's Task Force on Private Security developed a Standard calling for more research in the field. More specifically, it advocated that:

> The Law Enforcement Assistance Administration should encourage the development of a national private security resource and research institute. In addition, all universities, companies, organizations, associations, and individuals concerned with private security should increase their efforts in private security research.[17]

In the commentary section, which accompanied this Standard, the Task Force elaborated:

> Throughout the work of the Private Security Task Force, the lack of research for and about private security services was appallingly apparent. Scant attention has been focused on research to alleviate obvious problems and enhance the effectiveness of private security in crime prevention and reduction. Unless a reliable research base is available, administrators will continue to be handicapped in their decisionmaking roles. To help alleviate the problem of lack of base data, all entities concerned with private security should initiate and increase their research in the field. Also, a national private security resource and research institute should be established to act as a center and resource for these research activities.[18]

These sentiments were largely reiterated several years later in the Hallcrest Report which was published in 1984

and is the latest authoritative study produced to date. Of the dearth of empirical knowledge in the field, the authors made the following comments:

> Altogether, security is not a body of knowledge with a strong research base. Of the hundreds of publications in security listed in the National Criminal Justice Reference Service catalog most contain technical information for the practitioner rather than empirical data or theory on Security, asset protection, loss prevention, or economic crime. In the academic and research communities, security tends to be regarded as a private adjunct to the public criminal justice system.[19]

They went on to indict most of that research which had been conducted, by pointing out that such efforts:

> . . . have consisted of market research or have yielded "soft" numbers rather than hard empirical data on the nature and size of private security. It is therefore extremely difficult to construct tight research hypotheses which can then be accepted or rejected on the basis of empirical testing.[20]

The report recounted a common theme that serious research was needed. Two related recommendations were put forth:

> A nonprofit Private Security Research Institute financed by government and private resources would be useful to monitor growth and trends in private security resources and technology, and perhaps to develop security standards, strategies, technologies evaluation techniques, and cooperative programs.[21]
>
> Empirical research should be conducted into the cost-effectiveness of specific security measures, or combination of measures, in combating various types of crime and loss.[22]

Some of the more recent textbooks on private security have also stressed the need for research. In 1981, O'Block made the following comments:

> The importance of research in crime prevention or any other field cannot be over emphasized. Real research in the area of crime prevention is almost nonexistent . . . Crime prevention theories with practical hypotheses need to be developed and tested in a vigorous and scientific manner so that there can be straightforward answers as to which practices work and which do not. This research should be written up following proper scientific methodology, but the conclusion section needs to be devoid of jargon so that practitioners in the field can have immediate benefit of the results of the research.[23]

Gallati further stated in 1983:

> It is obvious then than research was limited in 1976, when the Task Force Report was written. Sad to relate, it is still very limited . . . The most urgent need in private security is the accumulation of meaningful data and analyses of the various activities that security is addressing . . . A dynamic profession needs dynamic research, which we do not have at the present.[24]

There are a number of possible reasons which could be put forth to explain the lack of research in the field. Some of these include:

1) The field itself is still in its infancy and lags behind the public law enforcement sector by fifteen to twenty years in terms of growth and development as a profession.

2) Governmental policy and decisionmakers have largely failed to recognize the potential contribution of the private sector to crime prevention and control, concentrating their attention on the public sector instead.

3) Private security has been slow to develop as an academic discipline and is only now evolving into a bonafide area of concentration at many educational institutions.

4) A large portion of the industry operates on a for-profit basis and is reluctant to invest financial resources on research which does not produce tangible or foreseeable results (i.e., profits).

5) Various segments of the industry are actually in competition with each other and so are understandably hesitant to enter into cooperative projects or share internal data with potential competitors.

6) Historically, many practitioners in the field have failed to appreciate the value of and need for empirical research. There have also been relatively few people in the field with the methodological and research skills needed to conduct and/or consume meaningful studies.

7) With the demise of L.E.A.A. and the current national economic climate, public and governmental funding sources to support research are increasingly scarce. Furthermore, private funding sources have been traditionally reluctant to provide needed monies to private security research.

The significance of the last reason cannot be understated. There have been some attempts to develop research and development institutes in the private security field. However, they have failed due to an inability to secure the necessary "seed money" or start-up funds. For example: In 1981 and 1982, the School of Criminal Justice at Michigan State University was unsuccessful in several attempts to obtain initial funding for a private security research and training institute which would also serve as a national clearinghouse for technology transfer and information dissemination. Samaritan Health Center, the subject of this particular study, also attempted to secure start-up funds for a similar venture and was equally unsuccessful for three consecutive years.

As of this writing, no formal research and development institute for the private security field has yet been

successfully funded and sustained. The closest effort in this regard involves the American Society for Industrial Security (ASIS) Foundation, which is currently providing $30,000 for a variety of independent research projects.

WHAT HAS BEEN DONE

Rand Report

Only a handful of significant research studies have been conducted in the field. Three of them have already been mentioned. The first of these was the now famous Rand Report.[25] It was the pioneer study for the industry and was published in 1972. It had two major purposes: to describe the existing state-of-the-art nationwide, and to develop some model recommendations and regulations for improving the industry as a whole.

All segments of the private security field were addressed in the study with special emphasis given to security personnel. The study's goals were intended to do the following:

1) Estimate trends, in terms of fiscal expenditures, manpower, and equipment.

2) Describe current roles, functions, organizational structures, interactions, legal authority, and regulations.

3) Examine shortcomings in the field, such as major functional problems and abuses.

4) Evaluate costs, benefits, and liabilities.

5) Develop basic policy guidelines for governing the industry.

In order to achieve these goals, a vast amount of data was collected and analyzed. This data was obtained from:

1) Published documents.
2) Interviews with security executives and managers.
3) Survey questionnaires from security employees.
4) Survey questionnaires from regulatory agencies.

The findings and recommendations were published in five volumes which, in general, did not paint a particularly flattering picture of the state-of-the-industry. Specific recommendations were put forth in the following areas of concern:

1) Overall licensing and regulation.
2) Screening and training of personnel.
3) Firearms regulation and training.
4) Access to public police records.
5) Arrests, searches, and use of force.
6) Alarm industry standards.
7) Cost/benefit evaluations.
8) Technology transfer.
9) Research.
10) Enforcement for violations and abuses.

Task Force Report

The next major research endeavor was the President's Task Force Report,[26] which was published at the end of 1976 nearly five years after its predecessor. In many ways it was similar in scope and purpose to the Rand Report. However, it went far beyond that study in that it focused

heavily in comprehensive recommendations. In fact, it was the first significant attempt to codify formal goals and standards for the industry. Over ninety such prescriptive statements and their accompanying commentaries were set forth in eleven different topic areas:

1) Personnel selection.
2) Training.
3) Conduct and ethics.
4) Alarm systems.
5) Environmental security.
6) Relationships with law enforcement agencies.
7) Relationships with consumers of services
8) Education and research.
9) Regulatory agencies.
10) Licensing of security agencies.
11) Registration of personnel.

The Task Force Report has often been referred to by critics and academicians as the "Bible" for professionalizing the private security industry. Unfortunately, like its predecessor, the Rand Report, it has not always been as well received by security practitioners because of its overall criticisms of the field, (e.g., poor quality of personnel, training, compensation, etc.), its advocacy of external regulation and the potential economic impact on individual security agencies with respect to complying with many of the Report's standards (e.g., better pay, training costs, etc.).

Hallcrest Report

The third authoritative study on private security was the Hallcrest Report[27] which was published in 1984. This four-part report took another in-depth look at the security field. Its main purpose was to establish strategies for improving the industry's ability to prevent and control crime.

Several research questions were addressed in the report. They focused on the following:

1) The respective roles, functions, and contributions of both the private and public sectors in the war on crime.

2) The degree of cooperation between the private and public sectors.

3) The degree of competition and conflict between the private and public sectors.

4) Perceptions and expectations between the private and public sectors.

5) The scope and growth of private security.

6) The comparative state of resources available to both the private and public sectors.

The research techniques employed were generally similar to those of the two previous studies (i.e., surveys, interviews, literature reviews, etc.). However, the Hallcrest Report went beyond its predecessors in terms of analyzing the relationships between the public and private sectors. In this sense, it took a more systemic view of crime prevention and control. The security industry was implicitly regarded as a subsystem which interacts with

other subsystems (e.g., public law enforcement). The nature of those interactions became a focus of attention.

The findings of the study described a large and rapidly growing industry with great potential, but still in its infancy in many ways. A number of problem areas were identified in the relationships between the private and public sectors. Recommendations were put forth in a number of areas, such as:

1) Public, private, and community collaboration in crime prevention.
2) Research and program evaluation.
3) Police/security cooperation, and liaisons.
4) Information sharing between police and security.
5) Training and certification.
6) Licensing and regulation.
7) Police "moonlighting" in security.
8) Reducing false alarms.

These three studies provide an interesting longitudinal overview of the status of the private security field. When comparing and contrasting their findings and recommendations, a number of interesting observations become readily apparent. First, the private security field is massive in size and still expanding. Second, its potential contribution towards crime prevention and control is still largely under-recognized and underutilized, although, this is slowly changing. Third, it is struggling towards maturity, but with the exception of its technological aspects (C.C.T.V.,

access control, computerization, etc.), it still lags behind the public law enforcement sector, as a whole, in terms of professional development and growth. For example, many of the deficiencies and problems identified in the Rand and Task Force Reports were still apparent in the findings of the Hallcrest Report. Issues such as the quality of security personnel, training, licensing and regulation, research, and interfacing with the public sector were still unresolved (even though moderate progress in some areas had been noted). In fact, a majority of the standards of the President's Task Force had still not been adopted by significant portions of the security industry eight full years later.

Other Efforts

Other than these three major research efforts, there have been a handful of other noteworthy empirical studies conducted in the private security field. Some of them involve replication studies. For example, a small number of states and municipalities have emulated the nationwide endeavors just discussed with similar purposes, research techniques and findings.

Buikema also conducted an interesting graduate paper on legislation governing the security field in each state.[28] He found that existing legislation generally did not provide adequate safeguards and controls over the industry and that widespread adoption of the Presidential Task Force's Goals and Standards was slow in coming.

In 1981, Hollinger and Clark conducted a study with importance to the security industry.[29] This well publicized project attempted to measure employee theft in the work place. Thirty-five businesses in the retail, manufacturing, and healthcare sectors were targeted in the Minneapolis-St. Paul, metropolitan areas. Company executives were interviewed and approximately 10,000 employees were surveyed to determine theft levels and patterns. Anonymous admissions of theft were obtained and analyzed. Findings revealed a much higher theft rate among employee populations than was previously believed to exist. Replication studies by these researchers in Dallas, Ft. Worth, and Cleveland showed similar results.

Such revelations provided the industry some of its first "tangible" evidence about the real nature and extent of property crimes in business. Previous figures were most commonly subjective estimates without strong support. For example, the most widely circulated figures on theft in healthcare involved estimates of between $2,000 to $3,000 per bed per year in losses.[30] However, an empirical basis for these estimates could not be found by the author in any of the literature in which these figures have been quoted.

Sherman also produced three somewhat promising research oriented reports in 1984. In the first, a longitudinal study, an analysis of litigation trends and patterns related to crime and security was conducted for the period of 1958 - 82.[31] Data was collected on all cases

involving major monetary awards reported to the American Trial Lawyers Association during these years. A broad representation of private businesses and public agencies was obtained. The findings were not surprising. In summary, the study found that both the number of successful civil suits and the amounts of the awards per suit were skyrocketing at basically exponential rates. The most common torts were failure to provide adequate security and false arrest/detention by security personnel (both of which were serious concerns at Samaritan Health Center prior to its relocation).

Sherman expanded on the results of this study in another report which was more of a position paper than an empirical research study. Nevertheless, it did contribute to the body of knowledge in the field, by providing rational standards for determining the foreseeability of criminal acts and assessing the adequacy of security measures.[32] These standards encouraged the use of quantitative techniques in the analysis of risk and responses to it.

Sherman's third work also does not actually qualify as an empirical research study, but had direct relevance to such endeavors. It was presented at a conference by the University of Maryland as an agenda for conducting experiments in crime prevention in the security field.[33] More specifically, it described the utility of controlled experimentation in developing a body of knowledge that could aid security decisionmakers to evaluate the effectiveness of

their efforts. It also identified a number of salient research questions and provided sample methodologies and research designs which could be employed to answer them.

The aforementioned studies represent the bulk of the significant research efforts accomplished to date. Most other published empirical works in the private security field have been confined to either basic demographic surveys of the industry, compilations of security related statistics or technically oriented product evaluations. Furthermore, in reviewing the literature, the author could not find one example of research relating to program or planning models. In effect, the state of security related research seems to be at a level of discovering "where we are now" and has not yet evolved to the level of developing or evaluating methods for "getting where we want to be."

PROGRAM, PLANNING, AND SYSTEMS MODELS

It should not be surprising that the security literature is generally devoid of research dealing with planning models or conceptual frameworks. There has been very little discussion about them. While literature in the social and behavioral sciences literally abounds with theories, frameworks, and models dealing with program, planning, development, evaluation, operations, management, and general systems thinking, the private security field has been slow to adopt or assimilate many of the principles, methods or techniques associated with them. In fact, in the

course of this literature review of hundreds of texts, professional journals and articles, only a dozen or so references to such subjects were discovered. Instead the literature has primarily focused on the technical and industry-specific aspects of the field (e.g., personnel issues, technology and hardware, training, particular problem areas, etc.). It has largely ignored many of the generic, "higher order" concepts and issues such as systematic planning and evaluation, program management, and General Systems Theory.

One of the shortcomings of program management in the security field is that its basic functions have not always been well defined nor fully understood. Gallati tried to correct this by reintroducing Urwick's and Gulick's now famous conceptual scheme summarized by the acronym "POSDCORB."[34] In this scheme, management functions include the following:

Planning

Organizing

Staffing

Directing

COordinating

Recordkeeping

Budgeting

In somewhat similar fashion, Ursic and Pagano identified seven universal functions associated with security program management:

Planning

Organizing

Staffing

Directing

Controlling

Representing

Innovating[35]

While providing relatively comprehensive and similar descriptions of a security program manager's scope of responsibilities, these models do not emphasize the importance of evaluating as a distinct and vital responsibility. Furthermore, they provide little sense of direction, flow, or process.

Others have corrected such shortcomings. For example, security program management is viewed by Girard as a cyclical process consisting of three basic elements: planning, management and implementation, and evaluation.[36] Frisbie used these same basic ideas in a general planning model with numerous specific tasks organized around three distinct functions: crime analysis, program planning and development, and implementation.[37] Post and Kingsbury further expanded on those models by identifying a number of discreet and cyclical planning steps which included:

Risk Analysis

Set Goals

Develop Plan

Implementation

Evaluate Plan

Modify, if necessary[38]

The more sophisticated of the models, described above, imply that security program management is a continuous process of planning, implementing, and evaluating. They are useful as conceptual models. However, all of them lack the specificity and focus necessary to be useful as blueprints for action by practitioners in the field. They require operationalization in the form of more concrete planning and evaluation frameworks.

One of the most common of such strategies, appears in management literature and probably the most widely utilized in the healthcare field, is the Management-By-Objectives approach. This methodology is highly consistent with all conceptual models which identify program management as a continuous process of planning, implementing, and evaluating. The M.B.O. approach concentrates on goals, specific objectives, timetables, quantifiable end-results, and corresponding steps or procedures for achieving them. Unfortunately, in the security literature there have been only a few references to this approach, as will be discussed below.

In what is generally considered the authoritative text on hospital security, Colling has discussed the importance of organizing a security program's efforts around a formal mission statement and set of programmatic goals. In his view, appropriate focus and direction would involve the following:

MISSION - . . . the mission of security is to protect and serve the hospital, its patients, visitors, and employees . . .

GOALS -
1. Protecting patients, visitors, and employees from harm and reasonable fear of harm.
2. Maintaining an acceptable level of order, control, and safety in the various hospital buildings and on hospital grounds.
3. Protecting personal and hospital property from theft, misuse, and vandalism.
4. Conveying an image of professionalism and behaving in a way that is conducive to good hospital and community relations.
5. Enforcing the various hospital rules and regulations.
6. Rendering miscellaneous services, as needed.[39]

Unfortunately, Colling did not address the significance of translating a mission statement and its accompanying goals into more concrete, measurable objectives. However, Healy and Walsh have touched briefly on this area by stating that, " . . . general objectives for the security organization should also be established. Those objectives should

be considered when the planning is being done."[40] They also stressed the importance of quantifying desired results and superficially described this overall process as Management-By-Objectives without going into detail.

In a similar summary fashion, O'Block has described the M.B.O. approach as:

> . . . identifying the major areas of responsibility of each department and each individual within the department and defining specific standards of job performance or objectives to be met by each. At a later specified date, actual results are measured against the stated objectives to see if the desired objectives have been obtained.[41]

Likewise, Post and Kingsbury made the following comments:

> Security goals and objectives should be established and the type of security input that is to be furnished to the overall program should be determined prior to initiating the planning effort. Goals should be measurable in every case and should state what security would intend to accomplish as a result of having performed the various protective tasks.[42]

While such elementary overviews are useful in that they advocate a proven and systematic planning scheme for security programs, they offer little to prepare the practitioner for actually implementing the M.B.O. approach itself. Others have provided more appropriate and detailed discussions towards this end.

For example, Ursic and Pagano have viewed M.B.O. as a concept and way of thinking about the management process in which:

1) The superior and subordinate managers of an organization jointly identify their common goals,

2) Define each individual's major areas of responsibility in terms of the results expected . . ., and

3) Use these measures as guides for operating and assessing the contribution of each of its members.[43]

They further identified four major steps in the M.B.O. process:

1) Setting objectives

2) Establishing unit goals

3) Periodic performance evaluation

4) Comparing results with organizational objectives[44]

In addition, they stressed the importance of integrating individual priorities and performance within the context of the larger organizational aim and provided examples of how the M.B.O. approach could be applied in such a larger setting. Finally, they made the criticism that, while the process is relatively basic and straightforward, it still is largely underutilized by security practitioners.

In Girard's previously mentioned discussion of the program planning, implementing, and evaluating cycle, he also outlined the basic elements of the M.B.O. process in terms of goals, objectives, strategies, specific activities or tasks and timeframes. He demonstrated how these elements can be applied to the implementation and evaluation processes (without specific reference to M.B.O. itself) and

provided a useful format for doing so, which he termed "Detailed Information Concerning Program Implementation and Evaluation" form.[45]

In what is possibly the best treatment of the M.B.O. process, as it has been applied to the private security field, Lynch developed a concise but informative "primer" on conducting M.B.O.[46] In addition to the basic information covered by others (such as general definitions, explanations of goals, objectives, and strategies, delineation of the steps involved, etc.), he set forth specific detailed guidelines for writing objectives, identified prioritization schemes for those objectives (e.g., must-do, ought-to-do, and nice-to-do) and elaborated on the various discrete activities required for collaboratively implementing the entire process. On this latter point, he listed the following:

1) Goals should be established by top managers.

2) Middle management submits a series of objectives for each goal.

3) Top management selects objectives.

4) Final statement of objectives by middle management.

5) Middle management submits broad overviews of strategies for each objective.

6) Middle management develops detailed strategies.

7) Begin implementation.[47]

Further practical contributions, made by Lynch, included providing a series of questions for evaluating the utility

of the objectives being developed, distinguishing between M.B.O. and program budgeting, and discussing some of the common pitfalls experienced in the "real world" when implementing M.B.O.

Implicit in any thorough understanding of Management-By-Objectives is a general systems view of security and organizations alike. Unfortunately, literature on systems thinking in the private security field is even rarer than M.B.O. or general program models. While the term "System" is widely used (and abused), there has been little consistency as to how it is used or even defined. Its most common application has referred more to technology (i.e., hardware, computers, etc.) than to any General Systems Theory approach to organizations and problems as espoused by such leading proponents as Churchman[48] and Von Bertalanffy.[49]

A general systems perspective is particularly vital to the success of security programs for no less than two salient reasons. First, crime and preventable loss is a systemic problem which, as history has shown, cannot be solved by only one small segment of society acting "in a vacuum." Second, in the private sector, attempts to protect the environment without an understanding of and sensitivity to larger organizational priorities and functions, as a whole, have often rendered those efforts ineffectual, and worse yet, in direct opposition to business operations. The result has often led both to a corporate view of security as

a "necessary evil," which is to be tolerated only within certain limits, and a security practitioner's view of being a "pariah" without welcome access to top decisionmakers' planning efforts. Unfortunately, both positions are equally wrong and counterproductive to the overall health and well being of organizations.

The author could find no specific discussions of General Systems Theory in security related literature and only three brief allusions to applied systems thinking. The first came from Wyllie in his discussion of guard operations, where he viewed systems thinking as an ". . .in-depth analysis of the client's situation and requirements. This assessment is vital to the development of a plan of action for a total security concept."[50] Needless to say this oversimplified interpretation of the systems approach lacked sufficient elaboration and clarification to be meaningful in almost any context.

Ursic and Pagano have expanded somewhat on the systems approach and provided a more useful interpretation of the concept. They viewed security operations within a context which can be analyzed in terms of both psycho-social and economic-technical systems. In their scheme of things organizational security consists of:

> . . . a dynamic and open psycho-social and economic technical system designed to create a security awareness that fosters mutually acceptable patterns of attitudes, behavior, and relationships within organizational environments.[51]

This view is based on the premise that:

> . . . security, organizational, and management theories should recognize and accept contributions from all disciplines. Attempts to limit the interdisciplinary field of organizational security management to one viewpoint would restrict vision and the opportunity for continued research and learning.[52]

They also stressed the importance of organizing security programs on the combined knowledge derived from the behavioral sciences, jurisprudence, management theory, and technology with special attention to the role of people as " . . . individuals, members of tasks groups, and members of total organizational systems in the broad society . . ."[53] However, they too did not provide any further detailed attention to the overall concept of the systems approach as a practical, broad-based perspective within which to analyze and develop the entire security function.

Perhaps, the most insightful discussion of systems thinking can be found in the writings of Healy and Walsh who have described the purpose of the systems approach in security " . . . to obtain a comprehensive solution to a total problem."[54] While they focused on the technological aspects of security, they indicated that a total security system required at least three major components working in concert, "hardware, software, and people."[55] They further demonstrated how these three components could be applied in a theoretical security program.

While these few applied views of system thinking do have limited utility to security practitioners, they do not

contribute much towards a fundamental understanding of the systems approach in its entirety. Without such a conceptual grasp of the nature of security problems and their solutions, as well as the position a security program has within the larger organizational and societal settings, all efforts, no matter how well intended, will generally fall short of the mark, because the "big picture" is lost. In effect, it becomes an issue of "not seeing the forest for the trees."

SUMMARY

Private security is a topic about which much has been written but little said, at least from a scholarly point of view. There seems to have been nearly as much written about the need to conduct research in the field as there has been actually conducted. Most of the latter has been targeted on merely describing the state of the industry and its problems. Little has been written about experimentation, research and development, or theory building.

These shortcomings are particularly ironic in light of the fact the size and scope of the private security field far exceeds that of all the public criminal justice sector in terms of human, technological, and fiscal resources. It would appear that the field is now at an equivalent stage of development that the public sector found itself in just prior to the passage of the Omnibus Crime Control Act of

1968. Unfortunately, it is confronted with the increased crime related problems of the 1980's.

Another unsettling fact about literature on the security field is that it is largely devoid of references to conceptual and program models, specific planning and evaluation strategies, and general systems approaches. This results in a very narrow perspective from which practitioners must function. The consequence is that they must rely on their own personal experiences or resort to "reinventing the wheel" in the development and ongoing management of their individual security programs. They simply do not have access to a broad-based body of knowledge upon which to professionalize the industry.

Scholarly literature in the healthcare security sector (the author's own chosen vocation) lags even behind that of the rest of the field. Efforts to correct this have been slow in coming. For example, over the last eight years, various healthcare security proponents have unsuccessfully attempted to fund and develop a private training and research institute which could also serve as a clearinghouse for technology transfer. As International Healthcare Security and Safety Foundation (I.H.S.S.F.) came into existence in 1981 for the purpose of promoting training, professional credentialing, and research. However, to date the research component has yet to be developed. Furthermore, the generation of a nationwide statistical database only reached fruition in 1987 after several years of debate

and discussion. Its first set of figures are only now being published and disseminated.

On a more optimistic note, two literary contributions, not previously discussed in this chapter, have been published in the healthcare security field by the author himself. The first of these was a textbook on hospital security management which was completed for the Michigan Hospital Association in 1983.[56] It contains a chapter on the ACTION MODEL, which itself will be discussed further in the next chapter of this dissertation. Second, an article on a model systems approach to healthcare loss prevention was published in the Journal of Security Administration in 1981.[57] A revised version of that model will also be elaborated on in the next chapter.

FOOTNOTES

[10]William C. Cunningham and Todd H. Taylor, Crime and Protection in America: A Study of Private Security and Law Enforcement Resources and Relationships, Executive Summary, (McLean, VA: Hallcrest Systems, Inc., 1985), p. 15.

[11]Cunningham and Taylor, p. 14.

[12]National Advisory Committee on Criminal Justice Standards and Goals, Report of the Task Force on Private Security, (Washington, D.C.: Law Enforcement Assistance Administration, 1976), preface.

[13]James S. Kakalik and Sorrel Wildhorn, Private Police in the United States: Findings and Recommendations, Vol. 1, (Santa Monica: The Rand Corporation, 1972), p. vii.

[14]Kakalik and Wildhorn, p. 105.

[15]N.A.C.C.J.S.G., p. 26.

[16]N.A.C.C.J.S.G., p. 259.

[17]N.A.C.C.J.S.G., p. 263.

[18]N.A.C.C.J.S.G., p. 263.

[19]Cunningham and Taylor, p. 3.

[20]Cunningham and Taylor, p. 3.

[21]Cunningham and Taylor, p. 63.

[22]Cunningham and Taylor, p. 64.

[23]Robert L. O'Block, Security and Crime Prevention, (St. Louis: C. V. Mosby Company, 1981), p. 422.

[24]Robert R. J. Gallati, Introduction to Private Security, (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1983), p. 278.

[25]Kakalik and Wildhorn.

[26]N.A.C.C.J.S.G.

[27]Cunningham and Taylor.

[28]Charles A. Buikema, "A Survey and Comparison of Private Security Service Legislation in Force in 1981," A Masters Thesis, School of Criminal Justice, Michigan State University, 1981.

[29]John P. Clark and Richard C. Hollinger, "Theft by Employees in Work Organizations," (Minneapolis: University of Minnesota, 1981).

[30]These figures have been repeatedly quoted and updated by the International Association for Hospital Security in conjunction with the U.S. Department of Commerce.

[31]Lawrence W. Sherman and Jody Klein, "Major Lawsuits Over Crime and Security: Trends and Patterns, 1958 - 1982," (College Park, MD: University of Maryland, 1984).

[32]Lawrence W. Sherman, "Protecting Customers From Crime: Draft Standards with Commentary for Determining the Foreseeability of Crime and the Adequacy of Security on Premises Open to the Public," (Washington D.C.: Crime Control Research Corporation, 1984).

[33]Lawrence W. Sherman, "Learning What Works: A Draft Research Agenda on the Effectiveness and Adequacy of Security on Public Premises." A paper presented at the Conference on Security and Liability at the University of Maryland, 1984.

[34]Gallati, pp. 49-55.

[35]Henry S. Ursic and Leroy E. Pagano, Security Management Systems, (Springfield, IL: Charles C. Thomas, 1974), p. 174.

[36]Charles M. Girard, "Planning, Management and Evaluation: Important Tools to the Crime Prevention and Security Officer," Handbook of Loss Prevention and Crime Prevention, edited by Lawrence J. Fennelly, (Boston: Butterworths Publishers, 1982), p. 492.

[37]Douglas Frisbie, "Crime Analysis in Crime Prevention Planning," Handbook of Loss Prevention and Crime Prevention, edited by Lawrence J. Fennelly, (Boston: Butterworths Publishers, 1982), p. 530.

[38]Richard C. Post and Arthur A. Kingsbury, Security Administration: An Introduction, (Springfield, IL: Charles C. Thomas Publisher, 1977), pp. 670-671.

[39]Russell L. Colling, Hospital Security, Second Edition, (Boston: Butterworths Publishers, 1982), p. 104.

[40]Richard J. Healy and Timothy J. Walsh, Principles of Security Management, (Long Beach, CA: Professional Publications, 1981), pp. 40-42.

[41]O'Block, p. 430.

[42]Post and Kingsbury, p. 668.

[43]Ursic and Pagano, p. 191.

[44]Ursic and Pagano, p. 191.

[45]Girard, pp. 510-511.

[46]Ronald Lynch, "Management by Objectives," Handbook of Loss Prevention and Crime Prevention, edited by Lawrence J. Fennelly, (Boston: Butterworths Publishers, 1982), pp. 513-528.

[47]Lynch, pp. 520-521.

[48]C. West Churchman, The Systems Approach, (New York: Dell Publishing Co., 1968).

[49]Ludwig Von Bertalanffy, General System Theory, (New York: George Braziller, Inc., 1968).

[50]Joseph G. Wyllie, "Guards," Handbook of Loss Prevention and Crime Prevention, edited by Lawrence J. Fennelly, (Boston: Butterworths Publishers, 1982), p. 385.

[51]Ursic and Pagano, p. 38.

[52]Ursic and Pagano, p. 38.

[53]Ursic and Pagano, p. 38.

[54]Healy and Walsh, p. 200.

[55]Healy and Walsh, p. 202.

[56]Robert A. Smith, Hospital Security Management, (Lansing: Michigan Hospital Association, 1983).

[57]Robert A. Smith, "A Systems Approach to Loss Prevention in Hospitals," Journal of Security Administration, Vol. 4, No. 2, 1981, pp. 23-51.

CHAPTER 3

THEORETICAL FRAMEWORK

INTRODUCTION

The author's ACTION MODEL provided the basic core of the overall theoretical framework, upon which this study was developed and conducted. In one sense the entire reorganization of the security program at Samaritan Health Center can be viewed as a field test of the ACTION MODEL itself. In this chapter, it will be described in full detail.

In addition, a number of other conceptual models and approaches with importance to this study will be discussed. They supplemented and enhanced the effectiveness of the ACTION MODEL. They include a:

systems view of hospital security programs,

modified management-by-objectives planning approach,

generic decision-making and problem-solving scheme, and

set of strategies for implementing planned change.

The reader will discover that the ACTION MODEL contains a number of elements which appear very similar to some of those presented in the previous chapter. In fact, it may very well seem at first glance that the MODEL is actually a generalized compilation of the concepts of Girard, Frisbie, Post, Kingsbury, et al., organized into a more comprehensive

and cohesive format. However for the record, this is not the case.

The ACTION MODEL was independently developed by the author as part of a larger instructional handbook on healthcare security management, written for the Michigan Hospital Association. It was solely derived from the author's own professional experience, general academic preparation, and personal views and perspectives. All similarities and common themes with other published models are entirely coincidental. Nevertheless, they should be interpreted as being mutually reinforcing from a conceptual point of view. In fact, these independently published positions actually provide a form of consensual validation for the author's own ACTION MODEL.

ACTION MODEL

The ACTION MODEL is based on the simple premise that the effective management of a hospital security program involves three distinct, but ongoing and cyclical Processes; namely, planning, executing and evaluating. These somewhat generalized concepts are translated into a number of discreet, but often interrelated Tasks (or activities). These in turn are further operationalized in terms of functional Components (or elements). These Components represent applied schemes, approaches, plans, concepts, etc.

It is these major Processes, related Tasks, and key

Components which constitute the building blocks of the ACTION MODEL. Each will be described and discussed below.

Processes

Planning. Planning is something that every security manager does to varying degrees, often without realizing that the manager is actually planning or else without fully understanding the exact nature of what is being done. The planning process itself addresses two basic questions:

Where do we want to be?

How do we get there?

The planning process can be conceived as a deliberate effort to organize, coordinate and direct the activities of an organization. As such, it is primarily a decision-making process. Proper planning is also goal-directed (i.e., oriented towards attaining some desired condition). Therefore it is future-oriented, proactive process.

Proactive planning, while necessary, is often not sufficient to deal with the variety of day-to-day problems and unexpected crises which emerge in an organization. This is because even the most sophisticated proactive plans can do no more than anticipate the future with some degree of probability. Such plans are based on future goals, given future sets of conditions or situations. Unfortunately, however, the future is not as predictable as we would always like it to be. Instead, it can be full of surprises, many of which are unpleasant. When these surprises take the form of operational problems, then

original planning efforts may not be adequate any longer. In fact, unanticipated problems which arise can sometimes totally invalidate a proactive plan. Therefore, proper planning efforts must sometimes be reactive or problem-focused in nature.

Most plans, associated with what is commonly called "crisis management," would fall into this latter category. While such planning is sometimes necessary, there has been a general tendency in the hospital security field to place too much emphasis on it, as opposed to proactive planning. When engaging in reactive planning, there is also a tendency to lose sight of the overall goals upon which proactive plans are based. This is especially true when a security manager is faced with repeated problems. The end result is "putting out fires" all the time, instead of avoiding or preventing them in the first place.

Ideally then, planning efforts should have the flexibility to be both proactive and reactive in nature. The initial planning activities should be proactive and goal-directed. The need for reactive planning should be anticipated and directed towards making the necessary corrections in initial plans, so as to still be able to satisfy the original goals. In other words, reactive plans should be oriented towards correcting immediate and foreseeable problems, while at the same time being as consistent as possible with future goals. What has commonly been called "contingency planning" is a step in this

direction. In contingency planning, a variety of future scenarios are envisioned and appropriate strategies are made for handling each one in light of the overall goals which have been set. The result is built-in flexibility and increased likelihood that successful outcomes will be attained.

Even contingency planning cannot anticipate every possible change in needs, circumstances and conditions, nor every potential pitfall that may occur in the future. Therefore, problem-focused reactive planning (i.e., after the fact) is still commonly necessary. Unless circumstances dictate that the original goals themselves be modified, the reactive plans must remain compatible with the initial proactive or contingency strategies.

There are a number of Tasks and Components associated with the process of Planning as it has been variously described above. The Tasks include establishing direction, setting goals, developing strategies, and formulating tactics. The corresponding Components consist of philosophy, mission, scope of services, goals, objectives, action decisions, performance plans, resource plans, sponsorship plans, and implementation plans.

Executing. Executing refers to the broad set of managerial behaviors and responsibilities undertaken to convert plans into results. It is the carrying out (or implementation) of plans, the managing of operations and resources, and the

coordination and control of day-to-day activities. In the simplest analysis it means:

Now that we know what to do, let's get going.

The duties, related to the process of Executing, consume the majority of time and effort associated with security management and represent the most visible aspects of a security manager's job. For all practical purposes, the entire process of Executing can be defined in the ACTION MODEL as encompassing all program-related actions not directly tied to Planning or Evaluating.

The Tasks which correspond to the process of Executing are activating plans, managing resources, coordinating operations, and maintaining relationships. The relevant Components deal with leadership styles, administrative skills, and technical expertise.

Evaluating. Evaluating, in its simplest form, is nothing more than answering the following two questions:

Where are we now?

Where should we be?

However, it has several additional applications, which are particularly relevant to hospital security management. It is the mechanism for identifying future needs, diagnosing current problems, measuring progress and ultimately determining if a program's plans are being executed in a manner that accomplishes the goals set for them.

An evaluation is basically divided into two parts; namely, data collection and data analysis. Data collection

is the procedure by which all the information, needed to measure performance, results or conditions, is identified and compiled. However, in addition to the determination of which data are most appropriate for subsequent analysis, there are two other considerations. The first is the ongoing monitoring of performance, results, conditions, etc. The second is the periodic feedback of the same or similar information at specific intervals. The security manager must not only know what kind of data to collect, but also when it should be collected.

Data analysis is the procedure by which the information collected is actually examined, manipulated, and evaluated to determine if the security program's plans are being successfully implemented, and if specific needs or problems are beginning to emerge. Data analysis must also be conducted both continuously and periodically as appropriate. This analysis should focus on four basic types of issues: behaviors, conditions, perceptions, and observable results.

The Tasks related to the process of Evaluating are assessing needs, diagnosing problems, and analyzing results. The Components consist of operations audits, physical surveys, opinion surveys, and records analyses.

Recycling. The three major processes of Planning, Executing, and Evaluating are distinct but not disjointed. Instead, they logically flow from one to another in a cyclical process, which is continuous and repetitive. In fact, the effective management of any security program

depends on the constant recycling of these individual processes. In Figure 3.1 the actual nature of this overall relationship is better illustrated.

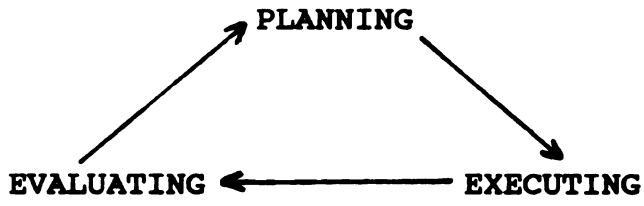


FIGURE 3.1
MANAGEMENT PROCESSES

It is important to note that in this nonlinear view there is no clearly defined starting point. In practice, however, a security manager must begin somewhere. While common sense might dictate that Planning should come first, the author contends that Evaluating is actually the first step in the cycle. Before meaningful plans can be developed and executed, there must be some notion of future needs, current problems or even more simply, the existing "status quo." Evaluating is the means by which such information is obtained.

Tasks

Within the context of each general Process, there are a number of related Tasks which must be carried out. In one sense each Process is actually defined in terms of its corresponding Tasks, which in turn are merely generalized procedures to follow. They are presented and described below.

Assessing Needs. As a prerequisite to proper proactive planning, attention should always be given to identifying foreseeable needs which have to be satisfied before desired end-results can be achieved (i.e., before goal attainment occurs). There must be some notion of the salient issues which must be addressed, anticipated variables which must be accommodated, and basic requirements which must be met. In effect, a security manager must know what the needs are, before the proper response can be formulated.

Needs can be viewed in terms of physical conditions (e.g., hazards), formal policies and procedures, informal attitudes, actual behaviors, program-related resources, and general organizational climates. When any of these dimensions manifests itself in such a way that it is counterproductive to or interferes with goal attainment; is necessary for goal attainment but lacking in part or altogether; or, is necessary but not in proper synchronization for optimal goal attainment, then a need is said to exist. Such a need must obviously be sufficiently addressed in the Planning process, but first it must be adequately identified in the Evaluation process. In fact, goal setting itself is largely dependent on the preliminary assessment of basic needs.

One particularly important feature of the entire concept of needs assessment is that it focuses on the future (hence is consistent with future-oriented, goal-directed planning). In this regard, it is intended to anticipate

and predict the future in terms of the "potential problems" described above, as they might adversely impact upon desired results.

Diagnosing Problems. Contrary to needs assessment, problem diagnosis addresses itself to current ongoing difficulties or incidents which have already occurred. (As such, it is more relevant to a reactive planning mode.) Whereas needs assessment strives to identify "what might go wrong," problem diagnosis focuses on examining "what has already gone wrong."

A problem can be simply viewed as an unmet need which has manifested itself with undesired consequences. However, a distinction should be made between an actual problem and its corresponding symptom(s). When a crime or security-related incident occurs, a problem is said to exist. At a very simple level of analysis this can be considered true, but, at a more in-depth level that crime or incident can also be viewed as the manifestation of a deeper rooted problem (i.e., a symptom). For example, if an employee has his car stolen in a parking lot, then he obviously considers it to be a significant problem. On the other hand, the security manager can acknowledge the seriousness of the incident, but would do well to look for underlying or causal factors which allowed the theft to occur at all (e.g., inadequate lighting, lack of security patrols and parking attendants, etc.). Only by identifying factors such as these can the appropriate corrective

measures be subsequently formulated as part of the planning effort. In other words, problem diagnosis goes beyond the obvious to answer the questions: "What's <u>really</u> wrong?" and "Why?" (A more detailed explanation of the actual steps involved is presented later in the section on Decision-making and Problem-solving.)

<u>Analyzing Results</u>. Once needs and problems have been properly identified, then plans can be made and carried out to satisfy them. The ultimate test of such plans is whether or not they achieve the desired results. This in turn is measured by way of a results analysis (often called a program evaluation). In effect, its purpose is to determine if the security program is actually accomplishing its established goals and objectives.

Results can be expressed and measured in terms of both quantitative and qualitative indicators, such as:

crimes and security-related incidents,
people's perceptions and attitudes,
adherence to fiscal constraints,
services performed, and
monetary and personal losses.

Detailed documentation of these kinds of relevant variables is maintained over time and routinely analyzed to determine changes and ascertain trends. Not only does this process reveal "bottom-line" results, but, when used to its fullest potential, it can also measure short-term progress

and even provide insights into problem areas, which may have otherwise escaped scrutiny.

Establishing Direction. In order to keep from "going on a tangent," a security program should be developed around a general orientation or perspective towards both the people it serves and its own basic role. More specifically, an overall sense of direction should be established as a prerequisite to planning and execution. Such direction evolves from a philosophical view of the basic rights and character of all people, a clear understanding of the program's broad-based mission, and a delineation of the actual scope of services to be rendered (all of which are specific Components to be discussed later).

An overall programmatic direction can influence the attitudes, level of professionalism, sense of duty and collective identity of security personnel, and can clarify the coverall priorities, responsibilities, and institutional relationships of the entire program. However, this overriding direction must also receive more than just lip service. Once formalized, it must be indoctrinated into and internalized by the members of the security department. It must also guide and govern all the efforts of the program at all times.

Setting Goals. The Task of goal setting is a twofold endeavor. It involves both the formulation of desired end-results or conditions, which are generalized and somewhat broad in scope, as well as more specific individual

outcomes, which if achieved, will create those desired results. When formalized, they constitute the goals and objectives to be described later as Components.

A security manager will generally have a fundamental notion of what the desired conditions at the hospital should be (e.g., low crime rates, no assaults, etc.). However, these views should be further refined and more clearly articulated on the findings of needs assessments and/or problem diagnoses. In other words, the security manager should take a systematic look at all identifiable needs and problems, then develop a set of desirable, but realistically feasible, conditions and outcomes which satisfy them. It is toward these conditions and outcomes that all subsequent efforts are to be directed.

Developing Strategies. Once desired end-results have been established, the next step is to begin to determine how to achieve them. (This is where the conventional and somewhat over-simplified view of the planning process in hospital security often begins.) General approaches for action are developed within the context of the goals set and the overall direction established for the program. (These Components will be discussed as action decisions later.) An example of such an approach would be to restrict all visitors to a designated entrance which is monitored, and where they would be screened and receive visitor passes.

Formulating Tactics. After general strategies have been developed, then their corresponding operational details are

specified. More specifically, the actual procedures to be followed and steps to be taken are formally laid out. Referring back to the visitor example, these would include the actual duties, responsibilities, and procedures for the security officer who monitors the visitor entrance.

This Task involves more than just "who does what, where, when and how." It also addresses: the acquisition, preparation, maintenance and utilization of necessary resources; the development of institutional approval and support for the actions to be taken; and the logistical details associated with the smooth transition from the "status quo" to new operational procedures. In effect, it requires the creation of four distinct, but interrelated types of plans (i.e., Components which will be discussed as performance, resource, sponsorship, and implementation plans later).

Activating Plans. The first Task associated with the process of Executing is to put all the previously mentioned plans into action. While this step may be often taken for granted, its importance cannot be overstated. No matter how comprehensive and well laid-out plans may be on paper, they do not automatically translate into success by themselves. They must be carefully put into motion with considerable attention to detail. A security manager should not take such transitions for granted, but instead should actively and consciously make them happen (hence the value of a preconceived implementation plan to facilitate this

process). This, in turn, requires adequate familiarization with the plans both by those implementing them and those impacted by them, training where necessary, the appropriate scheduling and phasing in of various elements of the plans, ongoing monitoring, troubleshooting for unforeseen "roadblocks" and the flexibility necessary to make minor adjustments or modifications as dictated by circumstances.

Managing Resources. Once the mobilization of effort has been initiated, a security manager is ultimately responsible to ensure that the plans are carried through to fruition and executed as smoothly as possible, in conformance with the goals, objectives, and strategies upon which they were developed. This Task ordinarily consumes the overwhelming majority of a security manager's routine time and energy. It can be defined in terms of three general, but concurrent functions: managing resources, coordinating operations, and maintaining relationships.

Resource management deals with the ongoing developing and maintenance of all the security program's resources at hand, so as to maximize their ultimate potential and availability at all times. Resources can be generally defined in terms of people (e.g., security personnel), property (e.g., equipment, hardware, etc.), finances (e.g., budgets), and information (e.g., statistics, training materials, records, etc.).

This Task involves the adherence to all aspects of the previously developed resource plan. Furthermore, it

involves managing budgetary allocations, maintaining manpower levels and skills, keeping hardware and equipment in service, in good working order, and administering over information collection, storage and dissemination.

Coordinating Operations. This Task relates to the goal-directed functions carried out by the security program. Basically, it means that performance plans are executed properly. More specifically, it also means guaranteeing that assignments are appropriately made and completed in timely fashion, that all available resources are properly allocated and fully utilized at all times, that those resources are operating in synchronization with each other (as opposed to working independently or in actual opposition), and that personnel perform together as a team (instead of a group of individuals going in different directions). This in turn requires constant monitoring and oversight.

Another important aspect is maintaining steady two-way communications both intra-departmentally and inter-departmentally. Instructions and responsibilities must be clearly delineated and disseminated. Task-related feedback should be sought and provided. Constructive input should also be encouraged and accepted.

Maintaining Relationships. This Task takes into account the interpersonal dynamics of a security program within the context of a hospital environment. Every security program has a social dimension within a larger social system called

a hospital (as explained in greater detail in the following section on Systems View). As such, the nature and quality of social relationships within this setting are important determinants in the ultimate success or failure of the program, regardless of how well it is otherwise planned and executed.

Working relationships, within both the department and the hospital, should be continually fostered and nurtured. The security manager is largely responsible to see that this occurs by actively promoting cooperation, mutual understanding, trust and support between the department and the rest of the hospital. The manager should also attempt to neutralize potential sources and types of resistance in a positive fashion. (A variety of techniques for this are discussed in the section on Implementing Change.)

Interpersonal conflict should be discouraged and prevented as much as possible. When this cannot be done, then it should be immediately addressed and resolved in a positive and open manner. Teamwork, as opposed to individualism, should be stressed and rewarded. Strong communication links, both formal and informal, should be maintained hospital-wide. "Win-Lose" situations should be avoided, if possible, and replaced by "Win-Win" outcomes whenever feasible. Finally, the manager should ensure that the department is responsive to the concerns and demands of the rest of the institution, and does not adopt a

"defensive" posture when confronted by criticism or complaint.

Components

Within the context of each Process and its associated Tasks there are a number of Components (or required elements) which complete the ACTION MODEL. Some may be appropriate to a single Task, while others apply to more than one Task. However, they are all grouped by the individual Process to which they pertain.

The Components represent generic categories of approaches, plans, techniques and applied concepts, which can be employed in the accomplishment of Tasks. They are presented and described below.

Operations Audits. Operations audits are useful tools for conducting needs assessments and problem diagnoses. They focus on security-related behaviors within the hospital in terms of both formal procedures and actual practices. They are performed by examining the existence of procedural controls (i.e., standards, countermeasures, etc.), the adequacy of those controls and the degree to which they are adhered. When a shortcoming is identified, then appropriate goals, objectives, strategies and tactics can be developed.

Physical Surveys. Physical surveys can also be applied to needs assessments and problem diagnoses. They address the actual physical conditions within the hospital in terms of potential or currently existing risks, hazards and vulnerabilities (e.g., inadequate lighting, locks, alarms,

etc.). They are conducted by inspecting the entire physical plant and campus of the institution, as well as by soliciting input from staff members. Once a need or problem is identified, its criticality (i.e., potential seriousness) and probability (i.e., likelihood of occurring) is determined, and appropriate corrective recommendations can then be made.

Opinion Surveys. Opinion surveys are also helpful for assessing needs and diagnosing problems, as well as analyzing actual results. They deal with the security-related perceptions, attitudes, concerns and fears of patients, visitors, employees and medical staff alike. They are often underutilized, but merit considerable attention for three major reasons. First, perceptions are reality! The consumers of security services not only need to be safe and secure, they need to feel that way. An effective security program must be sensitive and responsive to such needs. Second, nonsecurity members of the institution provide a potential resource for identifying needs or problems which might otherwise escape the scrutiny of security professionals. Third, the opportunity to be heard and provide input and feedback is conducive to healthy organizational relationships.

Such surveys can be conducted via interviews, written questionnaires, suggestion boxes, and telephone "hotlines." Results are then factored in with the findings of other evaluation techniques for subsequent attention.

Records Analyses. Records analyses can sometimes be used to assess needs or diagnose problems (e.g., looking at past crime rate trends in the hospital or police statistics for the adjacent neighborhood). However, its primary utility is in analyzing results (i.e., evaluating the success of the security program in terms of the degree to which its goals and objectives have been achieved). This requires the collection, maintenance, retrieval and comparison of relevant program-related information over set time periods (e.g., monthly, quarterly or annually). As much as possible this information should take the form of quantitative data and be directly related to and derived from the goals and objectives of the security program.

Traditional measures are often limited to crime and security-related statistics, but much more can (and should) be included. Some examples include actual monetary losses, budgetary compliance, complaints and commendations, miscellaneous services performed, and consumer opinions. There is no single and authoritative set of the types of records which merit analysis. Rather the rule-of-thumb should be to include all meaningful information upon which the formalized goals and objectives of the program can be evaluated.

Philosophy. A statement of philosophy is important in that it provides an overview of the values to be held paramount by the security program. It summarizes the overall security perspective on the nature of human beings in terms of their

inherent potential, rights, needs, value and social responsibilities. As such, it helps to define the overriding beliefs and general direction for the security program itself to follow. Furthermore, it can be utilized as a set of guiding and governing principles for all activities associated with the security program and all actions taken by its personnel.

Mission. A mission statement describes the security program's overall purpose for existing (i.e., its reason-to-be). It outlines the functional priorities of the program (e.g., to protect and serve) and puts into perspective its formal role within the hospital organization.

Scope of Services. A scope of services statement further defines a security program's role in terms of the types of services it is expected to provide within the context of its basic mission. It outlines the general duties and activities which are the responsibility of the program in the pursuit of its goals and objectives. In effect, it also sets the parameters for security operations and gives others an overview of what to expect from the program.

Goals. Goals are formalized descriptions of the overall desired end-results, toward which the security program's activities are directed. They represent the general conditions which will exist if the program is successful. They are the ultimate "targets" for all security-related efforts. (A more detailed description of both goals and

objectives will be provided in the section on Management-By-Objectives.)

Objectives. Objectives reflect and relate to goals, but describe more concrete end-results on a smaller scale. These tangible or measurable outcomes may be viewed as pieces or operationally defined elements of goals. (There may be several for each goal.) They make the achievement of the larger goals more manageable and are well suited to serve as practical benchmarks for measuring observable progress.

Action Decisions. Action decisions are the general strategies or approaches which are developed and employed to satisfy needs or solve problems. They reflect how energy and effort can be best focused and directed toward the accomplishment of objectives, the achievement of goals and the satisfaction of the security program's overall mission.

They constitute broadly defined plans, techniques, and actions which are to be carried out. Hospital and departmental "policy statements" often fall into this category.

Performance Plans. Performance (or work) plans are derived from action decisions. They assign the detailed and specific duties and responsibilities to individuals and groups of individuals. In effect, they are the actual tasks which must be performed as part of an action decision, and as such reflect all the operational elements of that

decision. Hospital and departmental "standard operating procedures" often fall into this category.

Resource Plans. Resource plans provide a support function for action decisions and performance plans. They involve the identification, acquisition, development, allocation and maintenance of all resources necessary to successfully execute an action decision or performance plan. Such requisite resources may include funding, manpower, equipment and hardware, orientation or specialized training, and general publicity or exposure.

Of all the resources necessary for a successful security program the most important is the human resource (i.e., people). While everyone in a hospital environment should have some role in security, the bulk of responsibility falls on the security department's personnel. Therefore, it stands to reason that considerable attention should be devoted to this particular group when resource plans are needed. However, maintaining a security staff at full operational readiness is one of the most challenging, time-consuming and complex tasks faced by a security manager, who is generally more of a security professional than a human resource professional. The manager may not even be familiar with all the various issues and considerations which factor into effective human resource planning. To assist this regard the basic concerns, questions and related issues associated with such planning are outlined below.

BASIC CONCERNS	RELEVANT QUESTIONS	RELATED ISSUES
Determining Manpower Needs	(How do we know the kinds and numbers of people we need?)	
	1. What services should we be providing?	Philosophy, Mission, scope of Services, Goals, Objectives, Action Decisions
	2. What kinds of work and tasks are required to provide those services?	Performance/Work Plans
	3. How can those tasks be organized and differentiated into separate groupings?	Individual Jobs
	4. What prerequisite knowledge and skill requirements are necessary to carry out the different groupings of tasks?	Job Qualifications (i.e., kinds of people)
	5. How many people are needed for each separate grouping of tasks (i.e., jobs)?	Manpower/Staffing Levels (i.e., numbers of people)
Satisfying Manpower Needs	(How do we go about acquiring and retaining the needed personnel?)	
	1. How do we attract the right numbers and kinds of applicants?	Recruitment
	2. How do we go about hiring only the right applicants?	Selection
	3. How do we keep only the necessary personnel on the job?	Retention, Separation

BASIC CONCERNS	RELEVANT QUESTIONS	RELATED ISSUES
Maximizing Manpower Potential	(How do we ensure the necessary quality of services to be provided?)	
	1. How do we appropriately cultivate the talents of employees to ensure desirable levels of performance?	Training and Development
	2. How do we accurately measure performance?	Appraisal or Evaluation
	3. How do we provide the proper economic rewards and incentives?	Compensation
	4. How do we correct and eliminate unacceptable behavior or less than satisfactory performance?	Discipline, Termination
	5. How do we provide the proper psychological rewards and incentives?	Motivation, Job Satisfaction, Morale
Utilizing Manpower	(How do we put manpower resources to the most effective and efficient use?)	
	1. How do we match the right people with the right tasks?	Assignment, Reassignment, Transfer
	2. How do we organize staffing levels according to varying priorities and demands for service?	Scheduling

BASIC CONCERNS	RELEVANT QUESTIONS	RELATED ISSUES
	3. How do we place available personnel according to their relative or potential contribution?	Promotion, Demotion

Sponsorship Plans. Sponsorship plans are detailed strategies employed to secure approval and sanction for proposed action decisions. More specifically, they involve the determination of who must be approached to receive formal (and sometimes informal) permission or support, as well as who might be expected to present significant opposition. Specific approaches are then developed to obtain the necessary approvals and to neutralize or overcome resistance. (A lengthy discussion of this entire process will be presented in the upcoming section on Implementing Change.)

Implementing Plans. Implementation plans consist of all the logistical and operational details necessary to put the other plans into action. They address the various issues, concerns, problems and steps associated with making a smooth transition from "past practices" to a "new way" of doing things.

Examples of some of the considerations to make in implementation planning include: scheduling and assigning, allocating and distributing, installing and/or removing, delegating and coordinating, orienting and training, setting timetables, anticipating pitfalls, and actively monitoring. The more complex, controversial or comprehensive the other

plans may be, the more attention is required for implementation planning.

Leadership Style. A security manager's leadership style is an important factor in how well (or poorly) a security program ultimately operates. Leadership style can be simply defined as the security manager's personal approaches and techniques for accomplishing positive results through others. It is the way in which the manager actually relates to others. This in turn reflects the manager's internalized beliefs and views on the proper structure and operational relationships of an organization, the appropriate role and functions of management, employee attitudes towards work, and the most effective means for motivating them.

Much has been written about these views in terms of differing models, theories and overall philosophies. In the final analysis, however, there is probably no single leadership style which is best universally. For purposes of the ACTION MODEL what is important is that the security manager develops and employs a personal leadership style which is both effective and appropriate to the general environment and specific situations. Otherwise the manager may find that the job is a constant "uphill battle" and that even the best laid plans will be difficult at best to successfully execute.

Administrative Skills. Another contributing factor to the success or failure of security department operations is the degree to which the security manager can exercise some basic

skills with respect to the overall administration of the program. More specifically, the manager must demonstrate the ability to: organize workloads, communicate effectively (both verbally and in writing), manage time, control expenses, maintain records, set priorities, schedule meetings, make decisions, purchase items, maintain equipment and property, make and justify budget or capital requests, generate and review reports/policies/procedures, and attend to a host of other routine and mundane duties.

The manager must also be able to effectively select, promote, assign, evaluate, train and discipline subordinates (as part of carrying out human resource plans), as well as generally monitor day-to-day operations and occurrences. Without such skills on the part of the manager, the security program cannot be expected to operate as efficiently as possible, nor realize its full potential.

Technical Expertise. In addition to sound leadership and administrative traits, the security manager must also be competent in his own chosen specialty area, namely, security. More specifically, the manager must be able to easily recognize and anticipate hazards and weaknesses, readily develop solutions and safeguards, know applicable laws and restrictions on security operations, keep up with evolving technologies and innovations, understand the uses and operations of security hardware and equipment, and be familiar with accepted operating procedures and techniques. In addition, the manager must know the routine duties,

responsibilities and tasks of all subordinate job classifications.

The majority of the Components described above have been presented in the form of applied techniques, approaches and concepts, which are necessary to the processes of Evaluating and Planning. However, the last three have been presented rather as traits, which are important to the process of Executing. These latter Components have focused on certain knowledge, skill and ability requirements of the security manager, but are also relevant to others (e.g., supervisors). Furthermore, they are all directly applicable to each of the Tasks associated with the process of Executing.

Summary

When all the Processes, Tasks, and Components are laid out in proper relationships to each other, they comprise the ACTION MODEL, as depicted in Figure 3.2. They are arranged in a generally sequential order. However, in practice, some of the Tasks and Components may overlap or occur simultaneously. Furthermore, the application of certain Tasks or Components may not be necessary in all cases (although they should always be addressed and considered for possible relevance).

The ACTION MODEL can be used as a guide both for the development of an entire security program (e.g., "from scratch") and for the satisfaction of smaller-scale individual needs and problems. It is comprehensive but

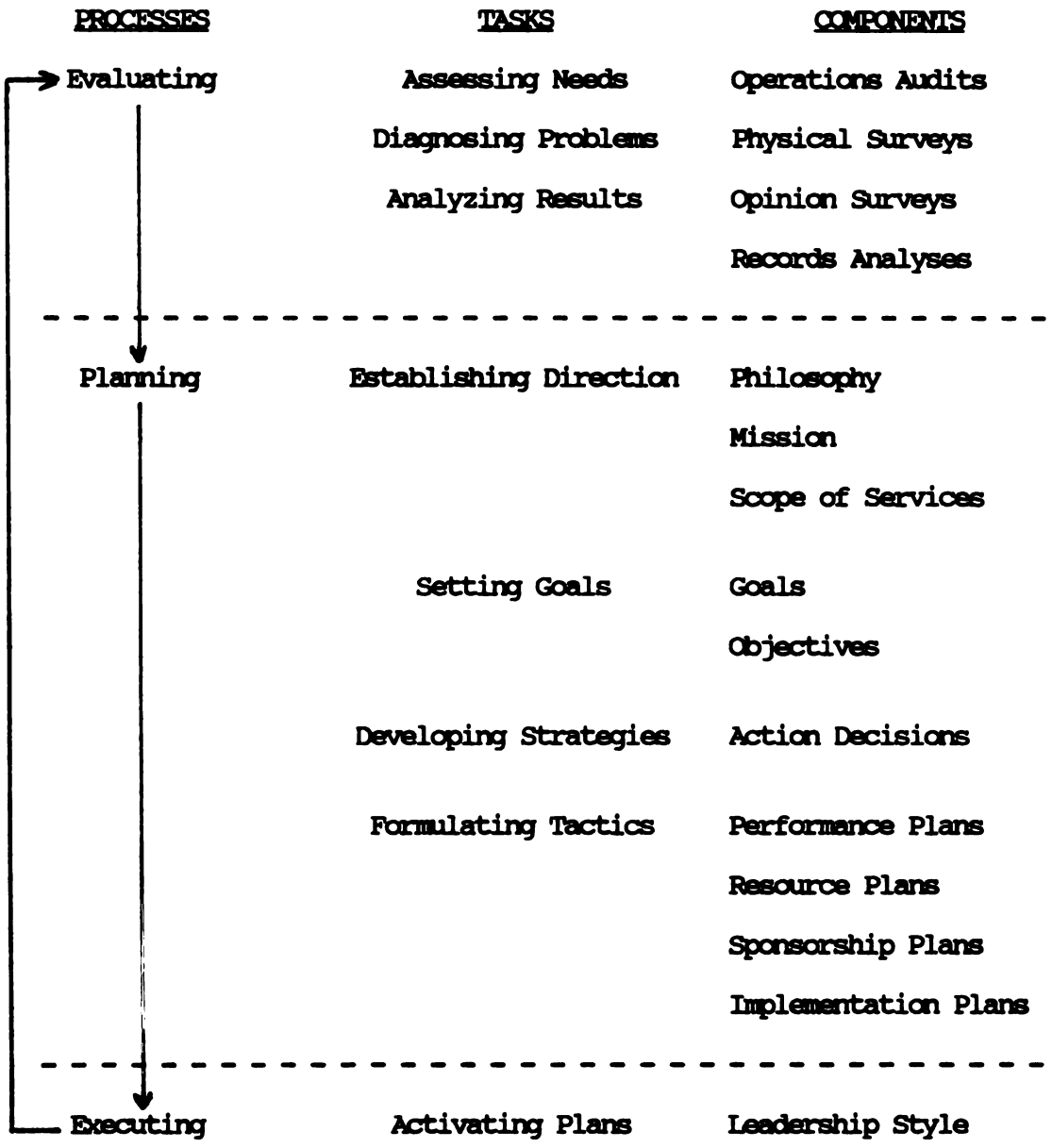


FIGURE 3.2
ACTION MODEL

relatively flexible. It has utility because it enables the security manager to organize and structure personal efforts, consider all major variables associated with a security program and determine appropriate starting points for action. It also serves to remind the manager that the overall management of a security program is a continuous, cyclical process.

All the principles, concepts and techniques presented in the remaining sections of this chapter can be readily applied within the framework of the ACTION MODEL. When employed together, they provide a very useful approach for the development and ongoing management of a successful and professional hospital security program.

SYSTEMS VIEW

The ACTION MODEL provides a practical method for determining how to conduct a hospital security program. It does not specifically focus on what kind of program to conduct. Before that can happen, the security manager should consider the potential form and function of the program from a systems point of view. No security program can be truly comprehensive and effective without some basic understanding and application of General Systems Theory.

Hospital security managers are often quick to point out that crime and security-related problems are both pervasive and systemic in nature. Unfortunately, not nearly as much attention has been paid to developing systemic solutions to

them. Instead, the norm has traditionally been to focus on immediate, emerging crises and treat them as if they occurred in somewhat of a vacuum (i.e., to put bandages on particularly troublesome symptoms instead of curing the larger problems). While progress has been made in recent years, the application of systems thinking in the hospital security field is still in the early stages of development.

Hierarchy of Systems

The General Systems Theory models, which have been variously applied to hospital security programs, can possibly be best understood in terms of those outlined by Buckley.[58] The first (and still most common) model to be adopted was the Mechanical Model,[59] which is most relevant to understanding electronic security systems (e.g., alarms, computerized access control systems, CCTV, etc.). However, this model is inadequate in explaining all the relationships inherent in a system of complex organizational processes and interactions, such as those which occur in a healthcare environment.

The Mechanical Model has come to be occasionally supplemented by a variation of the Organismic, or Homeostatic Model.[60] In following the logic of this latter model, a hospital can be loosely equated to a living organism. A limited range of crime and security-related loss can be expected and tolerated, while still permitting survivability of the system (i.e., continued existence of the hospital).

This Homeostatic Model is superior to the Mechanical Model in describing the less-than-exact and somewhat unpredictable relationships and interactions of an organization (as opposed to those of a machine), as well as their implications for security. In fact, it probably would be adequate altogether, if hospital operations could actually be examined without respect to human (i.e., social) considerations. However, hospitals are organizations of people. Many security programs, even those developed around a Homeostatic Model, fail to fully address the sociological nature of such organizations.

Few large scale efforts have been made to date which accommodate the fact that hospitals are social systems; that the causes and ramifications of crime and security-related loss are far more complex to deal with than ordinarily acknowledged; and that solutions to these problems must often originate on a social level, since that is where they occur.

Why is it so important to develop a security program upon theoretical tenets which specifically address human considerations and social interactions? It is the author's contention that the level and nature of crime and security-related loss is ultimately a function of the degree to which it is tolerated and accepted by the members of the system (e.g., the employees, medical staff, etc.). Conversely, the overall effectiveness of a hospital security program is at least, in part, a function of the level of acceptance,

support and cooperation of those same members. Therefore, no matter how well organized a security program may be on paper, it is doomed to some degree of failure, if the people who are affected by it (and in turn have an effect on it) do not participate nor support it. Furthermore, if a substantial number of people do not understand the systemic and social nature of crime nor actively contribute to the overall goals of the security program, then it can never fully realize its ultimate potential. The Mechanical and Homeostatic Models do not sufficiently address these realities. Hence, they are not the most appropriate models upon which to develop the most effective security program possible.

A more insightful model is the Process, or Complex-Adaptive Model.[61] While the previous examples focus on relatively simple and straightforward relationships on an impersonal level, the Complex-Adaptive Model envisions the hospital organization as a human organization (i.e., a socio-cultural system). Implicit in this conceptualization is an understanding that social systems are ". . .constantly changing and structure-elaborating,"[62] as opposed to being static or ". . .structure maintaining,"[63] as the Mechanical and Homeostatic Models would tend to indicate. The advantage of this approach is that it takes into account attitudes, motivations, changing values and how they all can impact on crime, as well as the status and character of efforts to combat it.

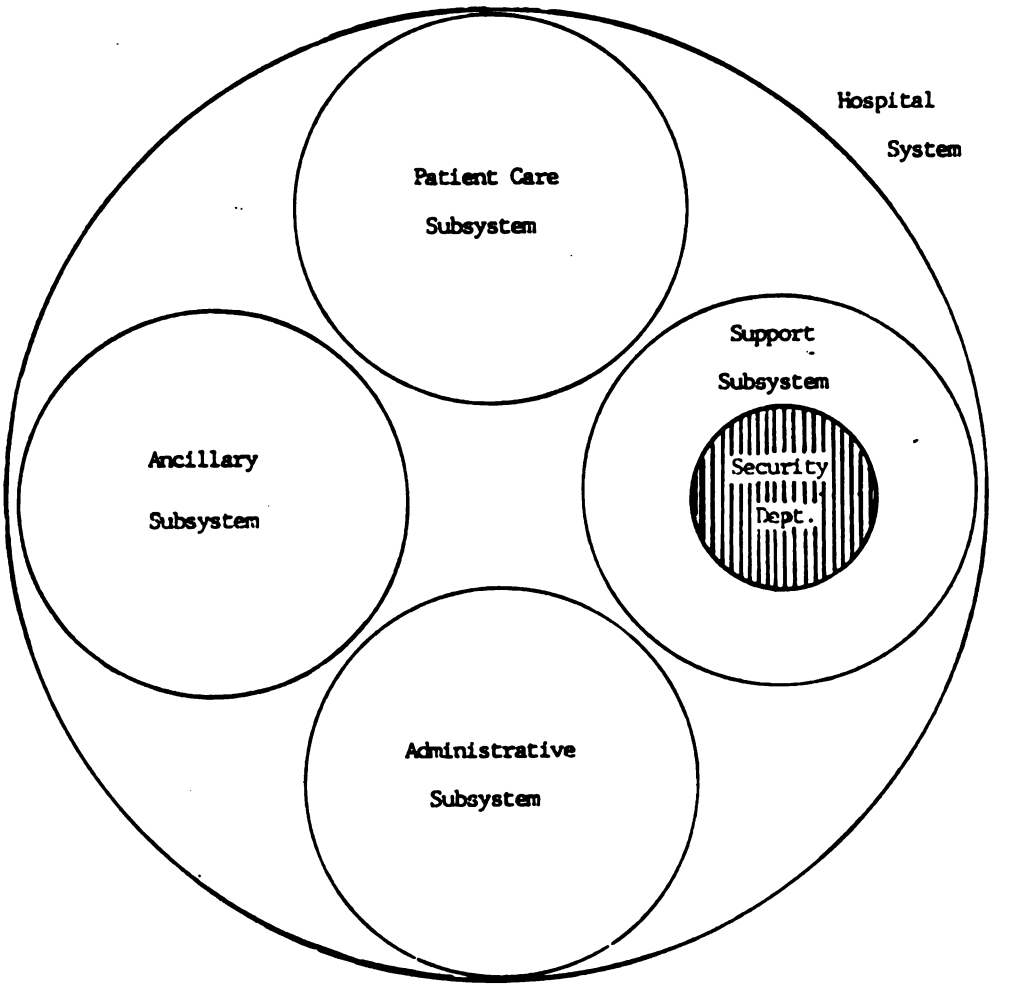
To be sure, certain elements of an effective security program can be understood in terms of a Mechanical Model, particularly the "high-tech" aspects. Furthermore, the Homeostatic Model is useful in describing how the viability of an organization depends on maintaining losses within certain acceptable ranges. However, in order to develop a truly comprehensive and successful security program, the social nature of both the problem and the organization itself must also be understood and factored into planning. People behaving and believing in certain ways create security-related problems: people behaving and believing in certain other ways can solve and eliminate those problems. Neither physical controls nor large numbers of security personnel alone are sufficient to accomplish the goals of a security program, without the understanding and involvement of the other members of the hospital. Therefore, the most appropriate conceptual model must be able to describe, incorporate and positively influence the social relationships within the institution, both formal and informal. A safe and secure healthcare environment can only be maintained by comprehending and taking advantage of the social nature of the organization, and by influencing values, attitudes, motivations and behavioral interaction (thereby actually changing the very nature and character of the system itself).

Security's Place Within The Hospital System

Hospital security managers who only subscribe to the Mechanical Model (or have no systems perspective at all) often perceive the hospital environment as merely "us-them-them" (i.e., security personnel, "bad guys," and everyone else). Proponents of the Homeostatic view may or may not share this position, but they do further distinguish the organization in terms of structural/functional components or subsystems, as depicted in Figure 3.3.

In this simplified model of the hospital system, there are four basic subsystems, arranged according to generic function or areas of responsibility. They are the Patient Care Subsystem (e.g., nursing, medical staff, etc.), the Ancillary Subsystem (e.g. respiratory therapy, radiology, laboratory, etc.), the Administrative Subsystem (e.g., administrative staff, accounting, planning department, business office, etc.), and the Support Subsystem (e.g., housekeeping, maintenance, food service, materials management, etc.). The security department would be a component (i.e., a sub-subsystem) of the Support Subsystem.

In this view of the hospital as a system, each subsystem has responsibility only for its own specialty area (although there is obviously some interaction between the subsystems). Linkage for interaction in or responsibility for security-related matters is largely nonexistent. Instead, sole accountability rests with the security department. Communication and interaction with other



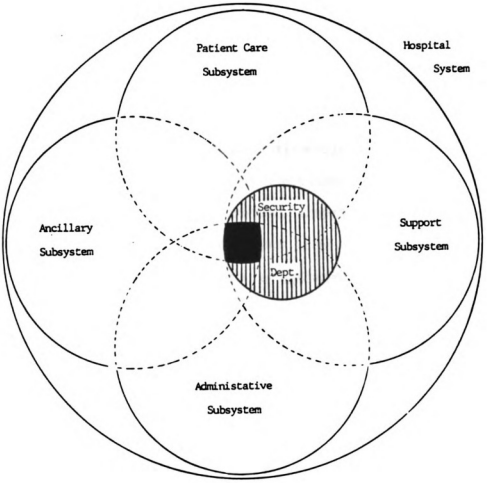
= Total Responsibility For Security (Security Department)

FIGURE 3.3
HOMEOSTATIC SYSTEMS VIEW

subsystems is generally one-directional and initiated by the security department. While security personnel are called when needed and complaints or reports of incidents are forwarded to the department, active cooperation must generally be solicited on a case-by-case basis.

This somewhat less than desirable state-of-affairs is often reinforced by the security department and the rest of the hospital alike. Security personnel tend to view themselves as "experts" in the field (which they indeed should be), and as such feel they know what's best for everyone else. Due in part to the high degree of emphasis on specialization in healthcare, others acquiesce to this view and consider security as "not my job." These mutually exclusive positions contribute to a couple of problems. First, a vast resource for providing a safe and secure environment is left virtually untapped. (After all if security is everyone's problem, shouldn't it also be everyone's concern?) Second, well-intended security measures can be naively imposed on the rest of the institution without respect to the practical and political ramifications they may entail. Whenever such measures interfere with other subsystem operations or are perceived as being restrictive or intrusive, then resistance may occur and make the effort ineffective at best and counter-productive at worst.

A different view of the hospital system, depicting the preferred relationships of its subsystems with respect to



= Shared Responsibility For Security (All Subsystems)

= Primary Responsibility For Security (Security Department)

Note: All other areas within dotted lines represent nonsecurity related overlaps and interfaces between subsystems.

FIGURE 3.4
COMPLEX-ADAPTIVE SYSTEMS VIEW

security is represented in Figure 3.4. It accommodates the social nature of a hospital and fits quite well within the Complex-Adaptive Systems Model. In this view, each subsystem still has primary responsibility for its own area of expertise, but there is some degree of shared responsibility for security-related matters. The focal point of this overlap is the security department, which still coordinates and provides overall direction for the effort. However, communications and interactions are system-wide, continuous and formalized. Mutual input, cooperation and understanding are both encouraged and facilitated. In effect, each subsystem assumes a personal role (albeit a small one) in its own security as well as that of the other subsystems, all under the general guidance and support of the security department. In this way, "the whole becomes greater than the sum of its parts" and the ultimate effectiveness (as well as social acceptability) of the security program is enhanced.

An Applied Approach

Hopefully, the preceding discussion has been conceptually useful in providing a general perspective. However, within this framework, a more operationalized approach for dealing with specific security-related issues is also necessary. Toward that end the author has developed the following "practical application" model.

At the most basic level of analysis the model has two dimensions: a Social Dimension which is defined in terms of

various system levels within the hospital, and a Security Dimension which is defined in terms of its system components. The two dimensions are aligned on vertical and horizontal axes to form a two-dimensional grid, as shown in Figure 3.5.

The Social Dimension consists of five discreet system levels, arranged in descending order of complexity. At the highest level of analysis is the Environment, which consists of the entire neighborhood or community adjacent to the hospital. The focus here is on the mutual relationships, interdependencies and interactions between the two. At the next level is the Institution itself, within the context of its functioning as a whole entity. Next is the level of Multiple Work Groups, which are actually distinct entities that tend to interact closely together due to shared or similar responsibilities, geographic proximity, common problems or mutual dependencies. Multiple Work Groups are interdepartmental (or inter-subsystem) in nature. Below this is the level of the Work Group, which is departmental or intra-departmental. Analysis at this level generally deals with department operations or interactions as a whole, but can also relate to separate shifts, individual job classifications or small groups of individuals working together. Lastly is the level of the Individual, whether employee, patient, visitor or physician. In traditional systems terminology, the Environment can be equated to a supra-system; the Institution is a system; and the other categories are various levels of subsystems.

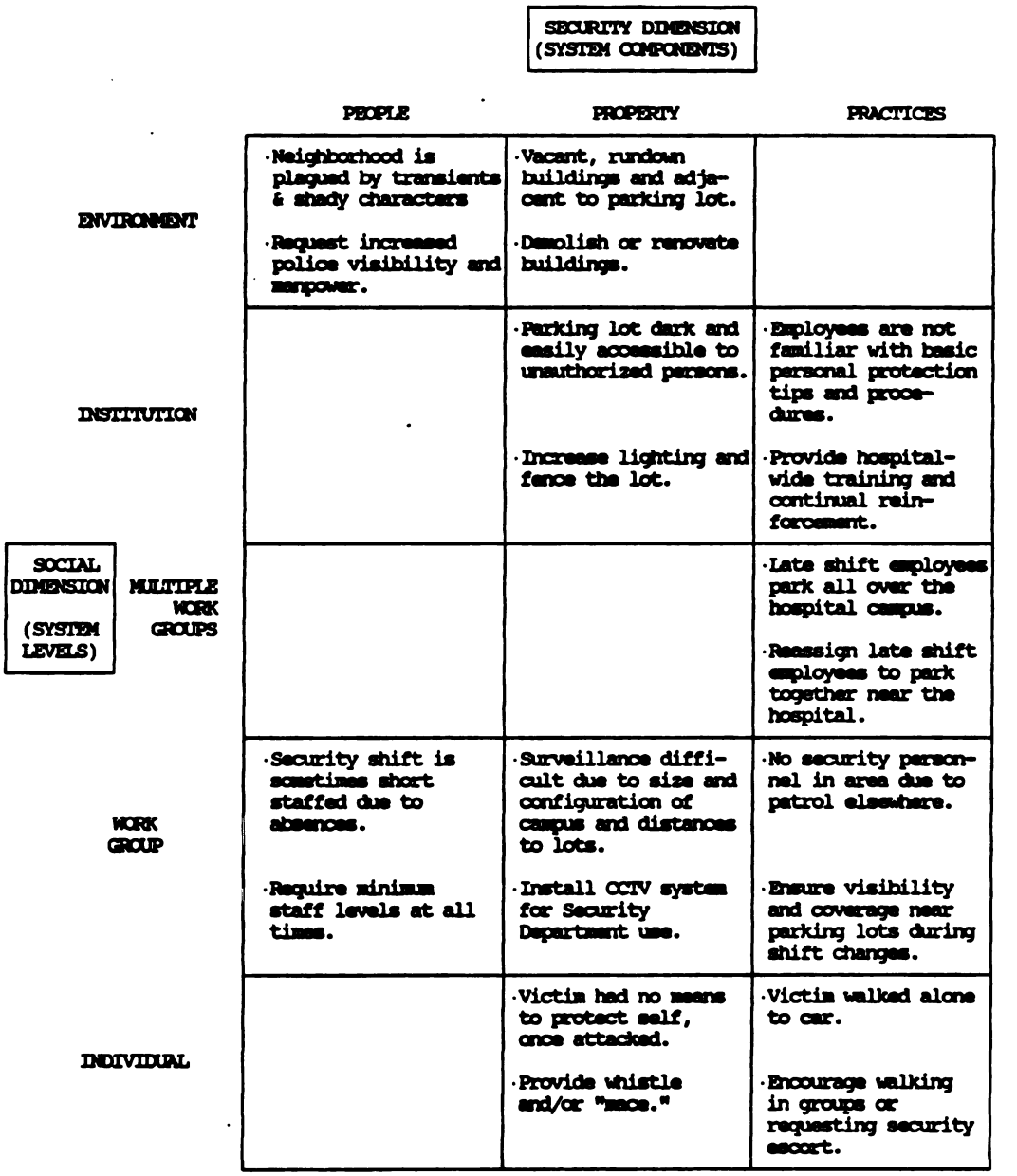


FIGURE 3.5
APPLIED SYSTEMS MODEL

The Security Dimension consists of three major components, which can be said to make up any comprehensive security program. The first component relates to People. Under the Homeostatic Model described earlier, the individuals of concern would be primarily security personnel. However, consistent with the Complex-Adaptive Model this category is expanded to potentially contain all persons within the hospital environment. The second component, Property, encompasses all the physical resource which can be applied to a security program (e.g., hardware, equipment, products, tools, buildings, structures, etc.). Some of the more familiar examples are CCTV, computers, alarms, locks, vehicles, radios, lighting, fencing and weapons. However, virtually any physical objective which can either create security hazards or enhance security conditions, falls into this category. The last component is Practices, or in other words the ways that people behave as related to security. This takes into account formal policies and procedures, rules and regulations, and requisite security-related information. However, the major focus is on the specific behaviors actually engaged in (or not engaged in), as opposed to those which are supposed to be engaged in (or not). Since there is often a difference between formal "policy" and real-world "practice," both must be taken into account, but emphasis should be placed on the latter.

Each of these components is highly interactive with the others. For example, people can use property in certain ways (e.g., monitoring CCTV equipment); people can behave in certain ways (e.g., following standard operating procedures); and property can affect people's behavior in certain ways (e.g., restricting access via keys or access cards). It is the nature of these interactions which either contributes to and detracts from a safe and secure environment. As a result, security breakdowns or problems can be analyzed and understood in terms of one or combinations of these categories. Likewise, corresponding solutions can also be formulated with their context.

In one sense these components make up a type of system in-and-of itself, with each one constituting a separate subsystem. The overall model, in turn, represents the merger of two types of systems, one social and the other security. Examination of any variable in one system is best made, when viewed within the context of some variable in the other system.

This applied systems model enhances understanding of the range of potential security-related considerations involved with the development of a hospital security program. It provides a useful tool for conducting needs assessments, problem diagnoses and the various steps associated with strategy setting and tactic formulation (as described earlier in the ACTION MODEL). This model itself does not identify specific needs, nor problems. Neither

does it provide specific solutions. (These can be reached by following the steps described in a later section of this chapter on Decision-making and Problem-solving.) It does assist the security manager in determining where to look for these needs, problems, and solutions. It forces the manager to consider all relevant possibilities in a structures manner, and focuses attention on where the needs and problems may exist and where the proper solutions can be best developed. In effect, the model constitutes a two-dimensional "checklist" for dealing with security related issues and concerns.

The following is a simplified example of how the model can be employed. Suppose a nurse gets off work late at night, leaves the hospital and walks across the street to a remote off-site parking lot, where she is assaulted and mugged. The security manager would respond to this unfortunate incident by trying to identify where a breakdown occurred in the security system (in terms of its various components) at potentially different system levels within the institution. The manager would keep in mind that there may be multiple problems at several different levels of analysis (as opposed to simply a single breakdown in one component at one level). In this way the manager would be better able to obtain the "big picture," as opposed to a non-systems thinking manager, who might be satisfied with only the most obvious explanation (e.g., the nurse

contributed to her own victimization by walking alone at night).

Once the contributing or causal factor(s) has been established in terms of a system component(s) at a certain level(s) of analysis, then the manager can begin to formulate the appropriate response to prevent a recurrence. The proposed solution(s) is relevant to and targeted at the same level(s) and component(s) where the problem(s) occurred. (Implicit also is a sensitivity to the possible social ramifications of any recommendations made.)

A number of sample causes and corresponding recommendations, which might have been established in the hypothetical example of the nurse, are provided in Figure 3.5. In each box is contained first, a possible contributing factor and second, a proposed solution. For simplicity's sake, there is only one cause and solution per box. In reality, there may be several. However, they still illustrate how the model can be successfully applied to a specific security-related case.

A Third Dimension

The model has so far been presented as two-dimensional in nature. However, there is a third dimension, which can also be incorporated into it (i.e., a lateral axis added to the grid, making it in effect a cube). This dimension is one of Time, more specifically broken down into three discreet time frames; namely, Before, During, and After a crime or security-related incident occurs.

The very existence of this dimension is implied in a needs assessment (i.e., identifying potential problems which have not yet occurred) and a problem diagnosis (i.e., identifying problems that have already occurred). It is also related to three important goals of any hospital security program (stated in the first chapter as the first three research questions). Succinctly these goals are: the prevention of crime and security-related incidents (i.e., before an occurrence), the minimization of harm associated with them (i.e., during an occurrence), and their correction or elimination (i.e., after an occurrence). However, consideration of the dimension of Time is most useful when formulating appropriate strategies, solutions and controls, in order to ensure a safe and secure environment.

In the example of the nurse above, one of the problems identified dealt with a breakdown in Practice at the Institutional level (i.e., the employees hospital-wide were not aware of the proper procedures and techniques to minimize their risk of becoming assault victims). The proposed solution was to provide institutional training in this regard. By incorporating the dimension of Time into this solution, the training could take three forms. One training component could stress such things as: walking in pairs, avoiding dark areas or potential hiding places, walking with confidence, carrying car keys, being alert, etc. Another training component could emphasize proper procedures to follow if attacked such as: self-protection

techniques, screaming, running, giving up one's purse, etc. Still another component could focus on such techniques as: positively identifying the perpetrator/vehicle/direction of travel, immediately reporting the incident, obtaining medical or psychological help, etc.

Another example at the level of the Work Group involving the Property component can be made. Suppose that the hospital pharmacy stores a large quantity of drugs in an accessible, but remote storeroom. The Director of Pharmacy fears that the drugs may be stolen. A number of physical countermeasures are possible. First, to prevent unauthorized entry into the storeroom, a lock or computerized card access system can be installed, with only select employees being issued keys or access cards. An alarm system can be installed to alert security personnel if the door is forced open. A CCTV camera hooked up to a VCR can also be installed to record a perpetrator for follow-up identification and apprehension. Each countermeasure described would be most effective in a different time frame, relative to the potential crime.

Summary

Hospital security programs do not operate in a vacuum. They are one component of a larger healthcare delivery system, whose subsystem components are both interdependent and interactive socially. Security programs, which fail to recognize and acknowledge that reality and tend to operate independently, will never be totally successful at best, and

quite easily can become considerable failures at worst. Further, hospital security managers who fail to grasp the "big picture" regarding the nature and scope of crime (as a pervasive social program), as well as its corresponding solutions, will always be handicapped in their effectiveness. They must appreciate the value of and operate from the systems points of view.

One applied approach to systems thinking examines security-related needs, problems and solutions, in terms of both system levels of the institution and major components of a security system, within the context of different points of time. It can be a very useful tool for organizing and focusing one's planning and evaluation efforts, identifying necessary variables for subsequent attention, and facilitating the development of comprehensive and appropriate strategies for action.

MANAGEMENT-BY-OBJECTIVES[64]

Management-By-Objectives is a systematized method of "program" planning, which is highly compatible with the ACTION MODEL, focusing on missions, goals, objectives, and action decisions. It can improve the quality of decision-making and problem-solving in the overall planning process by emphasizing results. More specifically it:

organizes one's thinking in a logical and systematic fashion,

directs that thinking towards the achievement of specific results, and

clearly defines those results and makes them as measurable as possible.

The M.B.O. approach has applications beyond merely planning. It can also be used to improve organizational climate, as a strategy in human resource development, and as a method of evaluating programs and individuals. For example, one of the basic principles of the M.B.O. approach is the joint or mutual planning between the security manager and subordinates or superiors. This type of collaboration promotes organizational communication, interpersonal trust, morale, and cooperation. M.B.O. also promotes the personal growth and development of subordinates by involving them as partners in the planning and achieving of organizational goals. It encourages their involvement and self-commitment and also allows them to make a greater contribution to the organization than just "following someone else's orders." This in turn benefits organization effectiveness as well as personal growth and maturity. Finally, it also provides an effective means for evaluating the overall performance and effectiveness of the organization, because evaluation criteria are built right into the program plans themselves. In fact, the M.B.O. approach actually provides the key component "Evaluation Plans" as an internal part of the overall program plans.

The Basic Elements of M.B.O.

The M.B.O. approach has several basic elements. They include:

1. Goals - Goals are desired conditions (or end results) that the security department strives to achieve.
2. Objectives - Objectives are the specific achievements that make up goals. In the M.B.O. approach these results are clearly defined (and preferably measurable) and can be compared to some standard or criteria within the context of a deadline. (In effect, goals and objectives together specify the "What" and "When.")
3. Action Steps - Action Steps are the basic tasks/activities necessary to satisfy Objectives. They are derived directly from Action Decisions (refer to the ACTION MODEL) and form the basis for Performance (or work) Plans for individuals within the department. (In effect, they specify "How."
4. Time Frames - Time frames are the periods designated for accomplishing the Action Steps. They are compatible with an Objective's overall deadline.

5. Review Dates - Review dates are the periodic timetables for monitoring progress and evaluating the action steps. They provide an opportunity to assess deviations from originally planned steps and to make necessary revisions or corrections along the way.

One useful formatting approach for organizing and structuring these basic elements is demonstrated in Figure 3.6.

Advantages of M.B.O.

The major attributes that can be associated with the M.B.O. approach are that it:

specifies the results to be attained,

specifies criteria for those results,

sets deadlines for accomplishing the results,

provides a built-in mechanism for monitoring and feedback, and

establishes personal accountability for the achievement of results (i.e., who is responsible for seeing that the results are attained).

Requirements for M.B.O.

In order for the M.B.O. approach to be effective, certain requirements must be observed. These include:

1. The development of as few goals as possible, all of which must be compatible with each other and representative of the overall departmental mission and philosophy.

2. The development of as few objectives per goal as possible. All should be compatible with each other and integrated in such a fashion that their combined achievement will satisfy their respective goal.

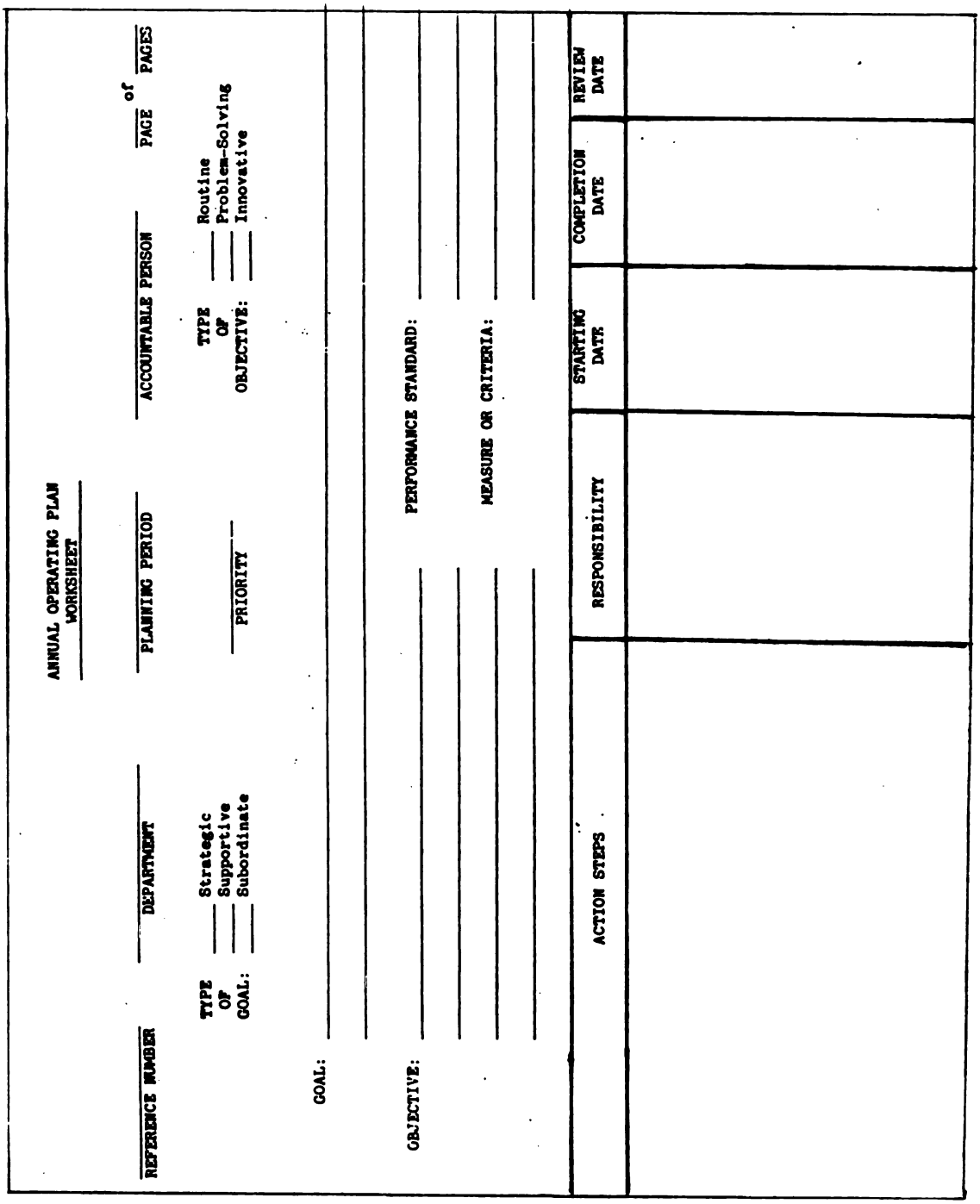


FIGURE 3.6
M.B.O. FORM

3. The setting of goals and objectives that are realistic, feasible, and within the means of the department to achieve. This excludes potential goals and objectives which are merely "wishful thinking" and not based on reality.

4. An emphasis on cost-effectiveness in the development of goals and objectives. In other words, developing those goals and objectives which will do the most for the least amount of money.

5. The formulation of these goals and objectives in writing.

6. Mutual agreement on the nature of goals and objectives between the security manager and subordinates or superiors insofar as they are jointly planned.

7. The appropriate prioritization of goals and objectives, such that the most important ones are satisfied first without unnecessary time and effort being expended on lesser goals and objectives (thereby possibly sacrificing the more important ones in the long run).

8. Simplicity and straighforwardness. Everyone involved should understand exactly the nature of the goals, objectives, and action steps, as well as their individual responsibilities for accomplishing them.

Types of Goals

Generally speaking, goals can be broken down into three major categories which can be described as follows:

1. Strategic (or Senior) - These goals are directly mission-related and are initially set by the security manager. They are high-order goals, governing the overall direction of the department.

2. Subordinate (or Line) - These goals are generally lower-order goals established by subordinates within the context of their own specific roles.

Achieving these lower-order individual goals contributes to the ultimate achievement of the strategic goals.

3. Maintenance (or Supportive) - These goals are focused on the optimization of the department's overall capability to satisfy Strategic (or Senior) goals. They deal with the acquisition, development, maintenance, utilization and retention of departmental resources, as well as communication, revenue generation and organizational climate issues.

Types of Objectives

There are three basic types of objectives which are relevant to the M.B.O. approach. They are relatively self-explanatory and can be described simply as: routine, problem-solving and innovative.

In addition, objectives can be further distinguished in terms of their measurement properties. In other words, some objectives are quantitative (and measurable) whereas others are nonquantitative (or qualitative). In M.B.O., the emphasis should be on developing objectives which are as quantitative as possible, although qualitative objectives are sometimes unavoidable.

Writing Objectives

In order to achieve maximum program effectiveness, objectives must be organized and structured along certain

lines. Generally speaking, an objective should be written somewhat as follows:

1. Start with the word "to,"
2. Followed by an action verb (e.g., decrease, increase, eliminate, etc.),
3. Followed by an expected result,
4. Followed by a standard/criteria (preferably quantitative in nature),
5. Followed by a date for completion.

Summary

Generally speaking, the M.B.O. approach transcends the structural hierarchy or an organization. In fact, many hospital administrators use M.B.O. in conjunction with their hospital security managers to plan the overall security program for that facility. However, even if M.B.O. is not the primary method for planning within a particular hospital setting, the security manager can still personally use M.B.O on his/her own initiative to improve overall planning effectiveness and provide direction for the security program. In this regard, it can be a very useful planning and evaluation tool for the security manager, even if no one else if involved in the process.

In most cases, best results will be obtained if the M.B.O. approach is also extended to include at least supervisors. In such a case, each individual supervisor will have his/her own set of personal objectives (based on Subordinate Goals), consistent with and supportive of the overall departmental objectives (and Strategic Goals). Even

security officers could be involved to varying degrees in this planning process, because of the potential value of their additional input as well as the personal commitment to be derived from increased involvement and participation.

As a word of caution, however, it would be appropriate the note that M.B.O. can be misused, therefore counter-productive, if it is not approached in the right fashion. For example, if a manager imposes M.B.O. on his/her subordinates and in effect tells them what all the goals and objectives are going to be, then ultimate success may be limited. This is because one of the basic principles of M.B.O., namely, participative management, has not been observed. When M.B.O. is used as a means for evaluating subordinate performance, the security manager must be particularly careful to avoid using this approach only to justify punishment when assigned objectives are not met (at least without providing corresponding rewards for when those objectives are met). Otherwise, the entire approach will probably never achieve the maximum desired results, because employees will not be committed to actually participate beyond what they are forced to do.

DECISION-MAKING AND PROBLEM-SOLVING

The ACTION MODEL, Systems View and M.B.O. Approach together provide a dynamic and comprehensive framework for the development and administration of hospital security programs. However, two basic cognitive processes are

required to bring everything to "life;" namely, decision-making and problem-solving. In fact, a security manager's entire job is largely one of making decisions and solving problems. Unfortunately, the actual steps involved in these processes are all to often poorly understood or else taken for granted. The result is "short cutting" and the whole quality of the decisions or solutions reached may then suffer.

In the author's view, there are a number of distinct sequential steps which should be clearly understood and adhered to whenever decision-making or problem-solving take place. These steps can be "plugged in" when appropriate, at any point in the ACTION MODEL to enhance the ultimate quality of a security manager's decisions and/or solutions. They are briefly discussed below.

Decision-making is the most basic mental activity that a security manager can engage in. Organizational and management literature contains a variety of models for decision-making. However, in the simplest analysis, the basic steps involved are:

1. Formulation of a <u>desired outcome</u> or result.
2. The selection of appropriate <u>alternatives</u> for consideration.
3. The selection of appropriate <u>criteria</u> (which if satisfied will lead to the desired outcome).
4. The actual <u>comparison</u> of the various alternatives to the criteria and each other (i.e., both absolute and relative comparisons).

5. The selection or choice of the best alternative, given the criteria.

Problem-solving is, in reality, just a special case of decision-making. Whereas decision-making is commonly associated with proactive planning, problem-solving is generally associated with reactive planning. While there are also a variety of models in the literature on problem-solving, the basic steps involved may be summarized as follows:

1. Symptom Identification
2. Problem Diagnosis
3. Decision Making

Symptom Identification is closely related to the general process of evaluating. In fact, it is through evaluating that symptoms are identified. This occurs when the desired condition, at a given point in time (e.g., a goal), is compared to the actual condition at that same point in time and an observable discrepancy in found. While there is a general tendency to label this observed discrepancy a problem, as often as not it is actually a symptom of some other, unseen problem.

Problem Diagnosis goes beyond mere Symptom Identification and in its simplest form can be described as follows: "What's really wrong?" and "Why?" After a discrepancy has been initially identified through preliminary evaluation (i.e., Symptom Identification), then it can often be viewed as merely a symptom of some deeper

rooted problem. When this happens, the next step is to identify the possible underlying cause(s) of that symptom. In other words, what caused the observable discrepancy in the first place?

Once these underlying causes have been also identified, then the next step is to determine the nature of those causes or the nature of their casual relationships (keeping in mind that seldom is there only one cause). The important question here is how do the underlying causes(s) lead to or result in the symptom.

The next step is to determine the reasons for those causal relationships. The major concern here is why do those casual relationships lead to the symptom.

Following this line of reasoning, in order to properly diagnose the real problem so that it can be solved (as opposed to merely treating the symptom), it is crucial that you answer the questions: What?, How?, and Why? This in turn means that you must be able to describe the symptom, explain what the underlying causes are, explain how the underlying causes interact, and understand why those causes interact the way they do. This is a basic prerequisite to proper problem-solving.

After the real problem has been properly diagnosed, the next task is merely one of corrective decision-making (which consists of the steps already identified). The various steps associated with these cognitive processes are summarized in Figure 3.7.

I. DECISION-MAKING:	A.	Determination of a desired OUTCOME
	B.	Selection of appropriate ALTERNATIVES
	C.	Selection of appropriate CRITERIA
	D.	COMPARISON of alternatives with respect to criteria
	E.	SELECTION of best alternative

II. PROBLEM-SOLVING:	A.	Symptom Identification
	B.	Problem Diagnosis
	C.	Decision-making

	Issue	Focus	Question
II.A. Symptom Identification:	DESIRED condition or progress at a given point in time — versus — ACTUAL condition or progress at the same point in time — equals — Discrepancy, which may be viewed as a SYMPTOM of some deeper problem	Describing	What?

	Issue	Focus	Question
II.B. Problem Diagnosis:	Identification of UNDERLYING CAUSE(S) of symptom(s)	Explaining	What?
	Determination of The NATURE OF CAUSAL RELATIONSHIP(S)	Explaining	How?
	Determination of the REASON(S) FOR CAUSAL RELATIONSHIP(S)	Understanding	Why?
II.C. Decision-making:	Same as outline above for I. B-E		

FIGURE 3.7
COGNITIVE PROCESSES FOR THE ACTION MODEL

IMPLEMENTING CHANGE

Hospital security managers quite often find themselves in a very frustrating predicament. They are expected to seek out and provide solutions to the security problems that exist at their respective institutions. However, when they develop and attempt to implement these solutions in the form of new security programs, the result is commonly failure. A proposed plan is either rejected, cancelled after a short period of time in operation, "watered down" so as to become ineffective, or simply unable to achieve its goals due to the lack of necessary cooperation. Furthermore, this happens in spite of the fact that the proposed change is specifically designed to benefit everyone by improving security conditions at the institution.

One obvious explanation for such failures can be attributed to poor quality on the part of the proposed programs themselves. They may simply be unrealistic or have little practical usefulness. However, even a well-planned program, incorporating the various principles within the ACTION MODEL, as discussed so far, can still ultimately fail if it doesn't receive the approval and support necessary to put it into operation, or if it encounters significant opposition from various segments of the hospital community that is not sufficiently neutralized.

The process of introducing security related changes in healthcare environments is examined in this section. More specifically, the key element in the ACTION MODEL called

"Sponsorship Plans" is addressed and an outline for successfully institutionalizing security proposals and recommendations is provided.

It will do so by focusing attention around two areas that are too often overlooked by security managers:

the social implications of proposed changes, and

the appropriate use of specific change strategies to obtain support for and overcome resistance to the proposed changes.

Theoretical Framework for Change

A hospital is much more than just a building where the sick and injured go to receive medical care. It is people--doctors, nurses, technicians, and a host of various ancillary personnel--all working together to provide that medical care. Given such a definition, a hospital can be further examined at two levels of analysis. First, there is a formal organization, consisting of established lines of authority (chain of command), division of labor and responsibility, highly structured communication networks, etc. However, a hospital also consists of an informal organization that includes personal leadership and influence, social and interpersonal relationships, communication "grapevines," etc.

Traditionally, security managers have sought approval for their proposals from primarily within the formal, bureaucratic structure of their institutions. This is a logical approach, because administrative permission is generally needed for large scale institutional changes

(e.g., mandatory I.D. badges for all employees, package inspections at all entrances, etc.). However, far less attention has been devoted to gaining popular support for proposals from the informal or social organization that exists within their hospitals. In other words, general employee support and voluntary cooperation is not actively pursued; instead, it is often naively expected without much question, if it is considered at all.

Failure to approach the social organization with a proposed security program can have adverse effects on the ultimate success of that program. This is due to the fact that most security-related change efforts (which generally require cooperation, compliance or participation on the part of the hospital employees) involve some form of social change, which may be broadly defined as:

> . . . relearning on the part of an individual or group in response to newly perceived requirements of a given situation requiring action, and which results in a change in the structure and/or functioning of social systems.[65]

This "relearning" will be a very slow and uncertain process, if the "newly perceived requirements" are imposed on the social structure of an institution by way of bureaucratic decree. Sower understood this and pointed out, in his Sponsorship Theory of Organizational Change,[66] that the informal organization can have considerable impact on the potential success or failure of planned social change. He has contended that a proposed change must not only gain the approval of Administration, it must also have enough

support and cooperation from the "masses" to sustain it. Furthermore, potential sources of resistance to it (e.g., union opposition, employee protests, petitions, sabotage, etc.) must also be sufficiently overcome or neutralized.

In effect, Sower has maintained that social change should not be something that is done to employees, but rather something that is done with them. However, getting the support of the social organization requires several steps in the overall change process. He has outlined these steps in his Model for Community Action.[67] For purposes of this section, three of these steps are particularly relevant:

1. Establishment of an Initiating Set.
2. Legitimation and Sponsorship.
3. Establishment of an Execution Set and Mobilization of Resources.

Establishment of an Initiating Set involves the bringing together of various influential people within an organization to consider a tentative proposal. Ideally, these people will represent both the formal bureaucratic structure (e.g., administration) and the informal social structure (e.g., union officials and social group "leaders"). The purpose of this Initiating Set is to agree upon a common group goal, which may be the initial proposal from the security manager or some variation of it. Once they have agreed on a goal, they become the main sponsors

of it, and attempt to promote it to the rest of the institution.

Legitimation and Sponsorship involves the process of carrying out a "promotional" campaign for the benefit of the rest of the employees. During this stage of the change process, the Initiating Set must analyze the target population (i.e., the employees who will be affected by the proposed changes) to determine which people are needed to actively sponsor the proposal, which people must generally approve of it, which people can remain neutral without affecting it, and which people will probably oppose it. After breaking down the organization into these groupings, the Initiating Set must target their efforts appropriately.

Establishment of an Execution Set and Mobilization of Resources requires the development of a group of people in the organization who will be called on to actually carry out the proposal. The Execution Set may contain some of the same people as the Initiating Set, but generally more people are brought into the picture. For example, proposed security changes will often be carried out, to a large extent, by members of the hospital's security department. The mobilization of resources aspect involves all the operational details of putting the proposal into action.

In summary, to maximize the chances of success for a proposed change in existing security conditions, a security manager needs to develop a suitable power base that includes influential members of both the formal and informal

organizations at the hospital. These people must actively promote the proposed change to the rest of the employees, securing approval from those whose informal support is necessary, and containing opposition from those who could conceivably undermine the attempted change. Finally, the necessary resources must be mustered and put into operation.

Obtaining informal sanctions for a proposed change should be one of the first and foremost concerns of the security manager. However, another very important issue cannot be ignored; namely, the appropriate use of change strategies. In fact, even by following basic steps outlined above, a proposed change can still fail if the initial sponsors use the wrong tactics or approaches to gain acceptance and overcome resistance. In other words, the fate of a proposed change depends not only on determining <u>who</u> needs to be approached, but also on <u>how</u> they are to be approached.

The inappropriate use of change strategies can have adverse effects at virtually each and every stage of the overall change process. For example, the wrong "sales pitch" during an initial presentation to Administration can result in outright rejection of the plan before it even "gets off the ground." Likewise, inappropriate strategies at any one of the three steps in Sower's model can also be counterproductive to the ultimate success of a proposal, especially if the approaches used are perceived as "rubbing people the wrong way" and "going right over their heads."

In fact, the manner in which a proposed change is presented to the hospital community can make all the difference between success and failure, regardless of how much attention is devoted to reaching the "right" people.

Change strategies can take a variety of different forms and can focus on many separate considerations. However, they can be organized into discreet groups or types that reflect certain emphases. Zaltman and Duncan have classified change strategies into four basic types, which are conceptually useful to hospital security managers. Which one to use (or which combination of them to use) in a given situation, will depend on a number of specific factors that will be discussed in later pages. The strategies themselves can be described as follows:

1. Facilitative
2. Reeducative
3. Persuasive
4. Power[68]

Facilitative strategies involve any effort that makes it easier for the target group (i.e., employees in the hospital) to implement its own change. In essence, such strategies are designed to assist people in bringing about a desired social change. A prerequisite to the use of facilitative strategies is the recognized need to do something about an existing problem and the willingness to make the necessary change.

Reeducative strategies are designed to provide a target group with unbiased, factual information about a proposed change. The main emphasis here is to rationally justify the need to change, as well as to outline the specific aspects of the proposed change in question.

Persuasive strategies are intended to appeal to the target group through emotional, biased, or otherwise subjective means. Objective evaluation of the merits of a proposed change by the target group is not a primary concern. Instead, the emphasis is on coaxing or swaying people over to "the other side."

Power strategies rely on the use of force, coercion, manipulation, or threats to obtain compliance on the part of the target group. Voluntary acceptance and cooperation are less of an issue than in any of the other strategies.

A couple of important points need to be made about the use of change strategies. First, they may have to vary throughout different stages of the change process. For example, when a proposed change is initially introduced, it may be most appropriate to use a reeducative strategy to provide the target group with knowledge about the exact nature of the problem and its possible solutions. If the target group does not accept the proposal based on factual information, then a persuasive strategy might be in order. If this still does not obtain the amount of support necessary, then a power strategy might become necessary to

ensure compliance until the benefits of the proposed change become obvious.

Second, multiple strategies at the same point in time may be desirable. Such an approach would be applicable when various segments of the target group are at different stages of acceptance of a proposed change. For example, Administration might be highly receptive to any changes that would improve security. In such a case, a facilitative strategy would be appropriate to show how the needed changes can be made. However, union officials might be somewhat suspicious of proposed changes involving security (fear of a "police state," etc.). A strong persuasive strategy could be used on them. Furthermore, the general employee population simply might not understand the full extent of the security problems that a proposed change is intended to eliminate. These people might need a reeducative strategy.

The two theoretical approaches which have been discussed so far, can be combined to create a very useful model for understanding the vital elements of the change process. In effect, this model can provide a hospital security manager with a conceptual framework, upon which to organize and plan. The model or flowchart itself, is depicted in Figure 3.8.

This model constitutes a "skeleton" for successfully implementing security-related changes in a healthcare setting. However, in order to bring the whole process to life, it is necessary to fill in the "meat." This, in turn,

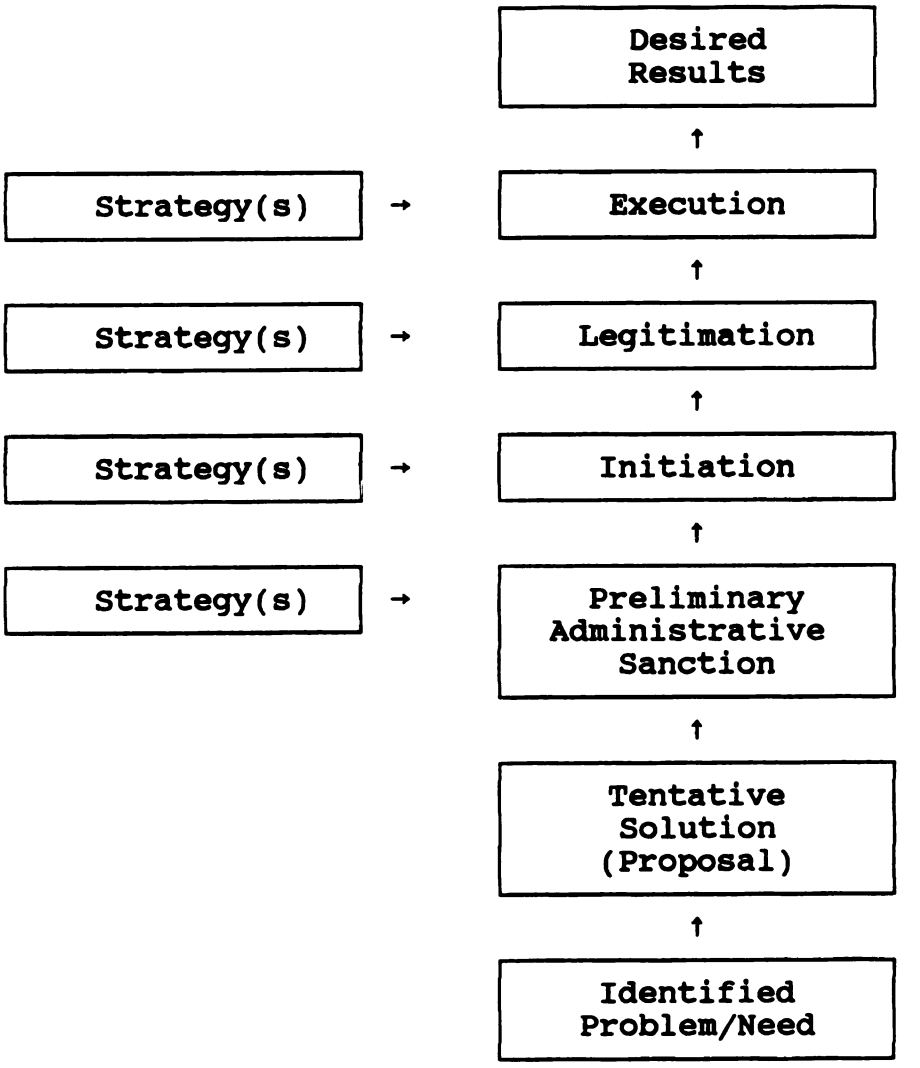


FIGURE 3.8
FLOWCHART FOR CHANGE

requires examination of the variety of factors, dimensions, and variables that come into play within the context of the basic framework described. The variables listed below make up a rough analytical framework, to be used within the context of the broader theoretical model. It is through the analysis of these "key" variables, that a security manager can ultimately organize and formulate a detailed plan for successfully institutionalizing security proposals.

Dimensions of Social Change

Any change process can be described in terms of a number of relevant components or dimensions. Warren has identified six basic dimensions that are compatible with the model used in this section. They are:

1. Change Objective (What is the desired outcome of the change effort?)
2. Target Population (Who will be the object of the change effort, both at formal and informal levels?)
3. Change Agent(s) (Who will be actively developing and implementing the change effort?)
4. Resistance (What kind of opposition can be expected and from whom?)
5. Change Strategies (What specific means will be necessary to overcome opposition and obtain approval?)
6. Stabilizing Effects (How will the change effort be sustained, once implemented?)[69]

Three additional dimensions, not stressed by Warren, but considered extremely important by Sower, should also be considered:

7. Change Components (What are the specific operational elements of the change effort?)

8. Relevant Relationships (What is the nature of the interactions between participants in the change effort?)

9. Historical Perspective (What has happened in the past that might affect or have impact on the current change effort?)[70]

Each of these dimensions should be considered by a security manager as a prerequisite to actually introducing the proposed security changes to the hospital. By identifying specific variables that pertain to each of these dimensions (e.g., who the change agents will be, what segments of the hospital population will be directly and indirectly affected, etc.) the manager can develop a foundation upon which to subsequently organize his/her efforts and get a better "handle" on the overall change process.

Most of these dimensions can be explored with little relative difficulty. However, some of them will require considerable data collection and analysis. Two in particular (change strategies and sources of resistance) will probably necessitate more detailed scrutiny, as discussed below.

Situational/Organizational Factors as Determinants of Change Strategies

Determining which specific strategies to employ depends on a multitude of situational/organizational factors and considerations, far too many to do justice to in this section. However, some of the most important ones have been

identified by Zaltman and Duncan and have been summarized for each specific type of strategy as follows:

STRATEGY	OPTIMAL CONDITIONS FOR USE
Facilitative	1) The target group: Recognizes a problem, agrees on the need for change, is open to assistance, is willing to work. 2) Top management is truly committed to the change. 3) There is little anticipated resistance.
Reeducative	1) Time is not an important issue. 2) Resistance may exist, but is merely based on misinformation. 3) Future resistance is possible, but can be immunized against with prompt action. 4) There is a need for the target group to be made aware of: the problem, cause/effect relationships and possible solutions. 5) The target group lacks the necessary skills to implement the change. 6) Strong commitment and compliance are not necessary for the change.
Persuasive	1) There is low commitment to change. 2) The target group is unwilling or hesitant to reallocate the necessary resources for change. 3) The problem is not fully recognized, and objective approaches do not look promising. 4) There is strong resistance to change. 5) There are time constraints. 6) Direct control over the target group is difficult to maintain. 7) The change is relatively complex. 8) The credibility of the change agent or sponsors is low.

Power	1) Compliance is necessary, but commitment is not. 2) The target group perceives a low need to change and cannot be persuaded to do so. 3) The target group refuses to reallocate necessary resources for the change. 4) There is a strong control over the target group. 5) A relatively small degree of resistance can be expected, and it can be overcome with firm action. 6) Change is vital and must be immediate.[71]

Determining which specific strategy(s) to use depends on any one or a combination of these situational/organizational factors. In some cases, these factors may conflict or even pertain to more than one strategy. Therefore, the security manager must develop sound insights into which conditions are most salient and then prioritize. Furthermore, he/she may have to probe even deeper into the political or social realities of the particular institution. This is especially true when addressing the issue of resistance, as the following will show.

Identifying Sources of Resistance

Perhaps the single most important prerequisite to determining the right strategy to use is to be able to identify potential opposition and resistance. This process requires the projection of:

1. Those individuals or groups who will be most likely to oppose a proposed change (e.g., nursing, second shift, minorities, etc.). "Who" will resist?

2. What type of resistance can be anticipated (e.g., grievances, protests, acts of flagrant disobedience, etc.). "How" will resistance occur?

3. The underlying reasons for opposition. "Why" will resistance occur?

By researching and understanding the relevant relationships that exist within the hospital and the historical basis for those relationships, a security manager should be able to anticipate most of these. However, the last consideration ("why") many present a particularly thorny problem, especially if there is no precedent for the proposed change or if the organizational climate is relatively unstable and unpredictable. In such a case, the security manager should concentrate on determining those factors which might breed opposition. However, in order to do this, he/she needs to be able to "know where to look." To facilitate this endeavor, Zaltman and Duncan have created a taxonomy of potential sources of resistance. This taxonomy, or outline, can be extremely useful in identifying the variety of different areas in which a security manager can direct inquiries with respect to determining why a proposal might be resisted. The basic elements or "barriers" in the outline are presented below:

Cultural Barriers--Strongly Held Values or Beliefs
Ethnocentrism
"Saving Face"
Incompatibility of a Cultural Trait with Change

Social Barriers--Group Solidarity (i.e., sticking together)
Rejection of Outsiders
Conformity to Group Norms
Inter-group Conflict ("They" like it, so "we" don't.)
Group Insight (i.e., limited perspectives)

Organizational Barriers--Threat to Power or Influence
Organizational Structure
Behavior of Top-Level Administrators
Climate for Change (e.g., poor timing
Technological Limitations

Psychological Barriers--Perception
Homeostasis (i.e., lack of tolerance for new inputs or arousal)
Conformity and Commitment
Personality Factors[72]

Warren has created a similar listing which overlaps to some degree, but also approaches the issue from a slightly different perspective. His classification scheme includes:

Habit

Disruption

Vested Interests

Ideology

Rational Conviction

Ignorance

Malevolence[73]

In summary, any one of these factors can account for or contribute to resistance. Quite often, a number of these factors come in to play. Therefore, a security manager should examine all of them closely, and use them as focal points for collecting and evaluating data to determine

potential sources of resistance that will have to be managed.

Necessary Conditions for Initiation -- Legitimation -- Execution

As already alluded to in the beginning of this section, there are a number of conditions that must be satisfied during each of the basic steps in the change process, as developed by Sower. These conditions are presented below as fundamental criteria to the successful implementation of proposed security changes or programs:

STEP	NECESSARY CONDITIONS
Establishment of an Initiating Set	Members of the set must have a socially defined "right to initiate" action (i.e., leadership at a formal and/or informal level within the organization). Members must obey the "rules of initiation" (i.e., the accepted norms for decision-making in the organization). Members must justify the need for change and agree upon group goals with respect to the proposed change. They must also actively sponsor the proposal. There must be internal organization with regards to the members (i.e., a working relationship). The members must have sufficient relationships with and access to others in the organization (i.e., those whose ultimate approval is needed) in order to effectively disseminate the proposed change. The proposed change must be compatible with the prevailing organizational definition of "public welfare.

	The goals established by the set must be realistically attainable and involve means which are appropriate (including the rules which specify the use of means.) The means must also be accessible.
Legitimation and Sponsorship	The initiating set must have access to the appropriate means for reaching people (e.g., mass media, newsletters, etc.) The initiating set must know who needs to be reached. More specifically; who must approve the change, who must actively sponsor it in order to mobilize the necessary resources, who can remain neutral without affecting the change, and who will oppose it. The initiating set must demonstrate that the proposed change will benefit everyone and not just its sponsors. The initiating set must gain popular support for the change from those whose approval is essential. The initiating set must neutralize any serious opposition to the change.
Establishment of an Execution Set	Members of the execution set must have a socially defined right to carry out the proposed change. Members of the execution set must have the appropriate means available to carry out the change (i.e., access to the necessary resources). The most important resource of all, the "fund of good will," must be mobilized and maintained.

> Members of the execution set must accept the goals that have been defined by the initiating set.
>
> Sponsors must not withdraw support for the proposed change, especially in the face of manageable opposition.[74]

While it is true that not all of these criteria must be satisfied for each and every proposed change, the failure to satisfy any one of them can undermine the entire change effort, depending on the circumstances and conditions that exist at a given hospital. Therefore, a security manager should pay special attention to each one of them and create a situation where as many as possible are satisfied.

Additional Considerations

Even if: all of the steps described in the theoretical model are followed, the proper strategies are employed, and sufficient attention is given to the identification of relevant variables, there is still no guarantee that a proposed security program will succeed. The best laid plans can often go astray. However, the purpose of this section is to assist hospital security managers in organizing a plan of action, so that their proposal will have a fighting chance. Towards that end, a few more miscellaneous suggestions would be in order.

1) Avoid rationalistic bias.[75]

Probably the biggest single mistake that security managers make during the development and presentation of their new security programs is to assume that the merits of

the programs will "sell themselves." In other words, security managers often expect to win approval for their proposals by simply laying out the elements of their plans and explaining the benefits that would be obtained from them. After all, how could any rational person reject a plan that makes sense and would improve security? Unfortunately, such a line of reasoning overlooks the fact that people do not always evaluate things rationally. Furthermore, objectively understanding the merits of a proposed program does not automatically mean that person will also be committed to it. Therefore, a security manager should carefully consider whether or not his/her enthusiasm for a specific change is shared equally by others. Employing different change strategies will help to ensure this, but there is still a potential problem that rationalistic bias will emerge under "the cover" of a large scale reeducative strategy. As a result, security managers would be well advised to ask themselves, "Am I assuming too much on the part of others?"

2) Do your "homework" before taking any action.

The need to collect relevant data and conduct research on one's own organization has already been mentioned briefly, but it cannot be stressed enough. In order to know such things as: 1) who should be included in the initiating set, 2) which strategies would be most useful, 3) what opposition can be anticipated, and 4) how the change effort can be stabilized and sustained, a security manager

must obtain information on such areas as: 1) the history of other change efforts at the institution (e.g., What went right or wrong?), 2) how various individuals and groups get along with each other (e.g., Will the unions oppose a change just because it's sponsored by Administration?), and 3) who the real leaders in the hospital are (as opposed to the "bosses").

There is no magic formula on how to collect and interpret all the right information. However, the variables described in this section do provide some basic guidelines on what type of information might be useful. The important point to note is that "knowledge is power." Have all of the facts at your fingertips, so that you do not go off "half-cocked."

3) Avoid personality conflicts.

Many attempts at social change fail simply because the participants spend more time and effort engaging in interpersonal conflicts than in actually trying to reach a consensus on what really needs to be done. The moment that personalities begin to clash over an issue is "the beginning of the end" for successfully resolving that issue. Therefore, keep disagreements at a professional level and leave egos out of the discussions.

4) Make the program's sponsors "look good."

Very seldom will people devote their best efforts towards a project for purely altruistic reasons. Personal motives are hard to avoid. However, the security manager

can take advantage of these personal motives and increase the vigor with which a proposed change is promoted by ensuring that the program's sponsors receive adequate recognition or positive "strokes." Anything that will enhance a person's credibility or social standing within the organization, will increase the chances that the person will be more committed to actively sponsoring a proposed change. This is especially important when dealing with Administration and the initiating set, upon whose backing the fate of the proposed change may well depend. Therefore, make sure that everyone who will be called on to help promote a proposed change receives credit for his/her efforts. A wise security manager will also realize that "our" proposal has a much better chance of success than "my" proposal.

In addition to these general procedural tips, there are some things that can also be done during the construction or "packaging" of a proposal. Zaltman and Duncan have outlined some dimensions or attributes associated with innovations. Each one of these dimensions should be considered during the preliminary development of a specific proposal. They are:

1. Relative Advantage (i.e., how well the perceived benefits of a specific proposal compare to the current "status quo" and other possible alternatives).

2. Impact on Social Relations (i.e., how much the proposal will alter the existing pattern of relationships within the organization, either positively or negatively).

3. Divisibility (i.e., the extent to which the proposal can be broken down into separate components and implemented on a limited basis or a little at a time).

4. Reversibility (i.e., the extent to which a proposal that has been implemented can be discontinued without creating additional problems).

5. Complexity (i.e., the amount of difficulty associated with understanding a proposal or putting it into effect).

6. Compatibility (i.e., the degree to which a proposal is consistent with existing values, belief or practices.).

7. Communicability (i.e., how well the proposal can be disseminated throughout the organization).

8. Time (i.e., the speed to which a proposal can actually be implemented within an organization).[76]

Ideally, a security manager should examine the preliminary proposal in light of these various dimensions, and then attempt to "fine tune" the proposal so that it:

1. Provides the greatest benefits possible in comparison to other alternatives.

2. Has minimal impact on existing social relationships within the organizations, unless newly created sets of relationships (as a result of the proposal) can be demonstrated to be better for everyone involved than the old relationships were.

3. Can be broken down into "smaller bites" and implemented a little at a time.

4. Can be discontinued if necessary, without creating more problems for the organization.

5. Is as simple as possible, requiring a minimal amount of effort with respect to understanding and implementing it.

6. Is relatively consistent with prevailing values, beliefs and practices within the organization.

7. Can be effectively communicated throughout the organization.

8. Can be implemented in an optimal amount of time, neither too fast nor too slow.

Practical Applications

So far, the reader has been provided with all the "pieces" needed to solve the "puzzle" of how to successfully institutionalize proposed security programs. However, equally important is the need to be able to put all the pieces together in a meaningful fashion. The following paragraphs will attempt to do just that, first with a brief overview and then with a more detailed checklist.

Trojanowicz has identified eight basic steps to follow in the development of criminal justice related change programs. These steps are:

1. Information Gathering
2. Analysis of the Organization
3. Relevant System Identification
4. Identification of Leadership
5. Bringing the Leadership Together
6. Identification of Consensus and Dissensus
7. Program Implementation
8. Quality Control and Continuing Program Development[77]

These steps are generally compatible with the basic model described in this section. For conceptual purposes they are useful by themselves, because they present a logical sequence of events in the overall change process.

However, they are also well suited to serve as broad categories of activities, within which the various elements of the model can be "plugged in." In this regard, a checklist of questions to be asked and steps to be taken is presented below.

1. INFORMATION GATHERING

   What is the exact nature of the change objective?
   What can it realistically be expected to accomplish?
   How is the change objective to be broken down into operational components?
   Who will be the primary change agents?
   Who will constitute the target population?
   What are the relevant sets of formal and informal relationships within the hospital and how might they affect the change effort?
   What is the historical background concerning change within the hospital?
   What situational/organizational factors exist that would affect the change effort or the use of specific change strategies?

2. ANALYSIS OF THE ORGANIZATION

   How will the relevant sets of relationships that have been identified affect the potential success of the change effort?
   What lessons can be learned from past experiences regarding change?
   How important are the various Dimensions in light of existing conditions at the hospital and how does the proposed change "stack up" against them?
   What is the overall potential for opposition to the proposed change?

3. RELEVANT SYSTEM IDENTIFICATION

   How can the target population be broken down into formal and informal groups?
   How will the various groups be affected by the operational components of the proposed change?
   What is needed from these groups with respect to the individual components of the proposed change? Understanding and acceptance? Commitment and participation?

Which groups and individuals are needed to actively sponsor the change?
Which groups are needed for overall approval?
Which groups can remain neutral without affecting the outcome of the change effort?
Which groups are likely to oppose or resist the proposed change?
Why will they resist it?
What type of resistance can be expected from them?

4. IDENTIFICATION OF LEADERSHIP

Who are the formal leaders in the organization and what is the extent of their leadership?
Who are the informal leaders in the organization and what is the extent of their leadership?
What roles can these people play towards the successful implementation of the proposed change?

5. BRINGING THE LEADERSHIP TOGETHER

Determine which strategy(s) would work best on Administration in order to gain their initial support for the proposed change.
Present the proposed change to Administration for approval, and make modifications if necessary.
Determine which formal and informal leaders should be included in initiating set.
Determine which strategy's would work best on the different members of the initiating set in order to gain their active sponsorship.
Make sure that the initiating set can satisfy the Necessary Conditions.
Make sure that the strategy(s) used on Administration and the initiating set conform sufficiently with the Optimal Conditions for Use.
Bring the members of the initiating set together for meetings on the proposed change.

6. IDENTIFICATION OF CONSENSUS AND DISSENSUS

Present the proposed change for discussion and feedback.
Identify areas of agreement.
Identify areas of disagreement and their underlying causes.
Revise the strategy(s) as necessary to resolve disagreements and any opposition that stems from them.
Establish and clarify group goals with respect to the proposed change, and modify the change itself, if necessary, so that it conforms with the final group goals.

Define areas of responsibility for the members of the set.

7. PROGRAM IMPLEMENTATION

Determine which strategy(s) are needed for the various segments of the target population in order to gain support and overcome resistance.
Make sure the strategy(s) used conform sufficiently with the Optimal Conditions for Use.
Direct the initiating set to begin promoting the proposed change (i.e., commence the legitimizing process).
Make sure that the legitimizing process can satisfy the Necessary Conditions.
Determine which groups and individuals should be included in the execution set.
Define areas of responsibility for members of the execution set.
Direct the members of the execution set to begin carrying out the proposed change.
Make sure that the execution process can satisfy the Necessary Conditions.
Determine which strategy(s) will be needed to ensure that the execution process will be completed satisfactorily.
Make sure that the strategy(s) used conform sufficiently with the Optimal Conditions for Use.

8. QUALITY CONTROL AND CONTINUING PROGRAM DEVELOPMENT

Collect data on how well the change is actually achieving the goals which have been established for it.
Collect data on employee attitudes towards the change, as well as the degree to which employees are cooperating with and/or resisting the change.
Analyze the various data collected to determine exactly how successful the change actually is.
Revise, update, and/or modify the components of the change effort according to the results of the analysis.
Determine what steps will be required to ensure that the change can be sustained (e.g., new and different strategies over time ongoing modifications, new members of the execution set, etc.)
Continually monitor the results of the change and any organizational/situational factors that might vary over time.

This checklist can be a very useful tool in organizing and directing the efforts of a hospital security manager who wants to implement new security programs. However, a number of caveats regarding its use are necessary. First, it is merely an outline and as such, cannot address each minute detail that must go into the development and implementation of a given security program. Such details are left to the security manager.

Second, the steps are laid out in an approximate order of occurrence. In reality, however, the order of some of them may change and many of them can (and in some cases should) be carried out simultaneously. In fact, depending on the unique situations that may exist at individual hospitals, some of the steps may have to be repeated or may not have to be carried out at all.

Third, there is still no guarantee that a proposed security program will be successfully implemented if the outline is followed. There are simply too many "unknowns and pitfalls" that may prevent ultimate success (e.g., the actual need for the program, its overall quality, environmental constraints, etc.). However, the chances for success will be greatly enhanced if the right steeps are taken.

Summary

Planned social change is an uncertain process at best. This is particularly true of chance programs that relate to security, because such programs involve not only the modification of behavior, but also the restriction of it to

some degree or another. Furthermore, security changes tend to have a reputation for being imposed on people, and so they are often viewed as "necessary evils" that should be avoided whenever possible. However, by acknowledging the social implications associated with new security programs and applying the most appropriate tactics to accommodate them, a proposed program will be far more likely to be favorably received by the people it is intended to benefit. Correspondingly, it will be far more likely to be implemented successfully.

CHAPTER SUMMARY

The models, principles, concepts and techniques, presented in this chapter constitute the overall theoretical framework upon which the hospital security program at Samaritan Health Center was developed, conducted and evaluated. In effect, the Samaritan program represented a field test of that framework. This research study provides an analysis of how well it actually worked in a real-world setting.

The framework is not intended to be the "last word" on how to conduct a security program. Instead, it merely represented one practical view. Neither is it meant to imply that the resulting form and function of the Samaritan program is necessarily best for all security programs. Rather, each separate program must be tailor-made to its own unique set of circumstances.

The framework is intended to bridge a gap between the academician (or theorist) and the practitioner. It has been developed to hopefully translate sound theoretical principles into an understandable and useful format for the security professional in the field. If it can accomplish that purpose, then it will have been a worthwhile endeavor.

FOOTNOTES

[58]Walter Buckley, Sociology and Modern Systems Theory, (Englewood Cliffs, NJ: Prentice Hall, Inc., 1967), pp. 8-40.

[59]Buckley, pp. 8-11.

[60]Buckley, pp. 11-17.

[61]Buckley, pp. 17-23.

[62]Buckley, pp. 18.

[63]Buckley, pp. 14.

[64]Much has been written about M.B.O. and as such, this section could abound with footnotes from various authors. However, general credit for this section will be given to George Odiorne, who is widely known as one of the leading proponents of the M.B.O. approach. With the exception of a few modifications and additions, which are of the author's own invention, the contents of this section were taken from a lecture by Dr. Odiorne, which the author personally attended in 1979.

[65]Gerald Zaltman and Robert Duncan, Strategies for Planned Change, (New York: John Wiley & Sons, 1977), p. 10.

[66]Christopher Sower, "An Experimental Sociology of Institutional Renewal," Rural Sociology, Vol. 41, No. 1, Spring 1976, p. 13.

[67]Christopher Sower, Community Involvement, (Glencoe, IL: The Free Press, 1957).

[68]Zaltman and Duncan, p. 60.

[69]Roland L. Warren, Social Change and Human Purpose: Toward Understanding and Action, (Chicago: Rand McNally Publishing Company, 1971), pp. 34-56.

[70]Christopher Sower, "Increasing the Effectiveness of Development Organizations." (A paper presented at the Asian Regional Seminar on Increasing Effectiveness of Development Organizations, 1980), pp. 6-7.

[71]Zaltman and Duncan, pp. 108-109, 132, 151, 165.

[72]Zaltman and Duncan, pp. 66-87.

[73]Warren, pp. 49-52.

[74]Sower, Community Involvement.

[75]Warren, Dennis, Changing Organizations, (New York: McGraw-Hill, 1966), p. 104.

[76]Zaltman and Duncan, pp. 13-15.

[77]Robert C. Trojanowicz, Juvenile Delinquency: Concepts and Control, (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1973), pp. 294-303.

CHAPTER 4

DESIGN AND METHODOLOGY

INTRODUCTION

This study can only be characterized as "unusual" by most standards related to typical Ph.D. dissertations for a number of reasons. First, it represents an Action Research endeavor which is often criticized for its lack of methodological soundness. Second, it largely requires the generation of its own internally developed data base as opposed to relying on existing data sources. Third, it involves the analysis of a wide variety of incident statistics and official records as well as opinion survey results. Fourth, its formal hypotheses are derived from action-oriented performance goals and objectives. Fifth, some of those objectives are not readily quantifiable.

Altogether, the study does not conform well to conventional norms for a methodologically sophisticated research effort. In its defense, however, it does systematically probe into a profession that has been basically unexplored in social science research and attempts to introduce accepted research principles into a "real world" setting, which often defies true experimentation.

The matters of data collection, analysis, and quantification will be addressed in subsequent sections of

this chapter. However, the issues of Action Research and hypotheses-versus-goals and objectives merit further discussion at this point. First, the general limitations associated with most Action Research studies are acknowledged. Such endeavors have been criticized on the following grounds:

> While attempting to be systematic, action research lacks scientific vigor because its internal and external validity is weak. Its objective is situational, its sample is restricted and unrepresentative, and it has little control over independent variables. Hence, its findings while useful within the practical dimensions of the situation, do not directly contribute to the general body of . . . knowledge."[78]

While such arguments are often true, they erroneously presuppose that Action Research cannot approximate more sophisticated quasi-experimental research designs. This is not necessarily an accurate assessment, especially with respect to this particular study. It is not contended that a true experimental design can be applied here, but some control over threats to validity have been exercised and will be discussed in the upcoming section on Research Design.

In addition to being an example of Action Research, this study represents an evaluation of an entire program which, according to the typology of Tripodi, Fellin and Meyer, would be categorized as a "quantitative-descriptive, program evaluation."[79] This type and subtype of social research commonly focuses on the evaluation of specific

program objectives as opposed to more formally developed hypotheses. More specifically:

> Such programs may contain a variety of objectives . . . Hypotheses may not be explicitly stated, and they frequently are derived from the objectives of the program being evaluated rather than from theory. Such studies may employ a variety of procedures to approximate experimental design.[80]

This description of program evaluations is particularly relevant because a Management-By-Objectives approach was employed in the reorganization of the security program at Samaritan Health Center. Furthermore, while this approach by itself is already generally accepted and practiced, additional efforts have been made to reconcile the program's action-oriented objectives with the more conventional format of research-oriented hypotheses. The common link consists of the reorganized program's overall goals, which formed the functional equivalent of formal hypotheses. They, in turn, have been accepted or rejected on the basis of the analysis of their individual operationalized objectives.

In the remainder of this chapter, the general research design and methodology employed in the study will be described, as well as the rationale involved. It is readily admitted that there are some inherent limitations relating to validity (and to a lesser degree reliability) largely as a result of the nature of the study itself, as well as a number of externally imposed constraints. However, it is also maintained that the overall approach represents a

definite improvement over current practice in the field and will hopefully permit the derivation of meaningful findings and results.

SAMPLE

The population of interest to this study varied slightly over the three-year period involved. However, it maintained relative stability and can be estimated at approximately 1,500 employees, 200 attending physicians, 150 vendors and service personnel, and 130 volunteers. Annual patient loads averaged 10,000 in-patients, 5,000 out-patients, and 38,000 emergency room patients. Visitors could be estimated at about 50,000 per year, thereby making the total figure of people requiring protection in excess of 105,000 per year. This protection was provided under the reorganized security program by a staff of approximately forty (40), including 26 "sworn" Specialists and Supervisors as well as 14 nonsworn Officers and Dispatchers.

Since Samaritan Health Center is an inner-city community hospital, the patient and visitor population was predominantly black, evenly distributed between males and females, and representative of all age groups. Volunteers were primarily black females. Vendors and service personnel were mainly white males. Physicians were mostly male and either black or of varied ethnic origins. Approximately, 78 percent of the employees were female and 52 percent were black or other minorities (e.g., Asiatic).

Three separate samples were employed in the study. The first consisted of the entire security department itself, both before and after the reorganization. Many of the individual security subjects, in this stratified sample, were not the same people from the pretest to the posttest phases of the study. This is because the reorganization effort itself involved considerable restaffing. In the year before the reorganization took place, the department consisted of 36 proprietary security officers and several rotating contract guards (which are not included in the study). Forty-five percent were black and 55 percent were white. Ninety-seven percent were male and three percent were female. One year after the reorganization there were 40 staff members, (excluding the author and secretary) over half of which were new employees. Forty-three percent were black and 57 percent were white. Sixty-eight percent were male and 32 percent were female. Staff composition in the second year after the reorganization varied slightly due to turnover, but was basically comparable in proportions to those of the first year. (More complete demographic profiles will be presented in the chapter on Implementing the Program.)

When making any comparisons between these pretest and posttest groups, the issue of nonequivalency (and all of its potential implications on validity) must be considered. To be sure, there are significant qualitative differences in the "calibre" and personal characteristics of the sample

subjects. However, within the context of this particular study, such differences do not necessarily impose serious methodological limitations. Instead, they are relevant and important factors because a major focus of the reorganization effort itself was to staff the department with more qualified, educated and professionally oriented personnel, who could theoretically accomplish the program's goals and objectives better. Analysis of the data, generated by these different groups, was intended to measure if that actually occurred (e.g., performance statistics, crime rates, etc.).

The second sample, involved in this study, was also stratified and consisted of all of the management personnel in the hospital (i.e., in-house physicians, administrators, department heads, managers, supervisors, and head nurses). While a randomized sampling technique of all hospital employees, volunteers, and attending physicians might have provided a more representative sample (and therefore enhance the generalizability of the results obtained), this was not "politically feasible." More specifically, the author's immediate supervisor would not permit large scale surveying of the entire population for a combination of reasons.

First, an independent and unrelated hospital-wide survey had been mailed to employees by the Labor Relations Department just prior to the onset of this study. Administration felt that an unnecessary proliferation of institution-wide surveys would not be in the best interests of the hospital during the transition period of its

relocation. Second, there was a general concern that too much public discussion about security at the replacement site would only heighten employee fears. Third, (and quite frankly probably the most important reason), Administration was more concerned with the views "at the top" so to speak (i.e., department head level and up). As a compromise, however, managers, supervisors, and head nurses were allowed to be survey sample subjects too.

This entire group varied from 172 to 138 people over the three years of the study. Approximately 33 percent were male and 67 percent were female. Sixty-eight percent were white and 32 percent were black or other minority. These percentages remained relatively stable. Mortality associated with turnover was less pronounced than for the security department sample. Most of the people involved with the pretest also responded to the posttests.

There was a third group of subjects whose input was relevant to the results of the study. This subset of the management team sample consists of the author's immediate supervisor, the Vice-President of Human Resources, and several other Administrators. While this group did not actually constitute a formal sample intended by the author, it was employed by the Vice-President himself to assist in evaluating the reorganized security program. More specifically, through the process of informal consensus, Administration decided to reach some of its own rather subjective conclusions on the success of the program. This

group is mentioned here because a number of the nonquantitative objectives (to be listed later in this Chapter) were evaluated by it. Their judgments formed the final decision on whether or not these objectives were individually accomplished.

The sampling techniques employed in this study did not ensure that a completely representative sample of the entire hospital population would be obtained. As a result, external validity (i.e., the generalization of results to all employees, volunteers, physicians, etc.) cannot be assured. This methodological weakness is acknowledged, and accordingly, any conclusions reached as the result of data provided by the sample groups will be qualified.

DATA COLLECTION AND MEASUREMENT

At the onset of the study, there was virtually no existing data base within the institution which could be used to develop research hypotheses or evaluate program results. Incident reports were seldom written. Crime statistics were not maintained. Employee opinion data had never been solicited. As a result, it was necessary to generate a wide variety of ongoing statistics, employing a number of different data collection techniques.

Two major data sources were utilized for subsequent analysis, department records, and survey questionnaires. Department records included the following types of information:

- Criminal activities
- Security related matters, incidents or activities
- Miscellaneous activities or services performed
- Turnover and absenteeism
- Budget figures
- Demographic profiles of incumbents

Most of this information was provided by the security department members themselves, either via formal reports or daily activity logs. The remainder was provided via various personnel records or institutional budget reports. This information was compiled over three time periods, from October through September, 1983 - 84, 1984 - 85, 1985 - 86. This coincided with the move to the replacement facility in October, 1984, and therefore provided comparable annual statistics before and after the move. (See Appendix A for a sample data collection form.)

Two primary survey instruments were administered. The first one was targeted for the security department sample and was designed to measure general progress over time. A number of questions were provided to measure the performance and leadership of the individual members of the management staff. Additional questions addressed the overall performance of the individual shifts as well as the general morale of the department. These questions were scored on one-to-ten (1-10) point scales with One equating to "Extremely Poor" and Ten equating to "Outstanding." Another type of question employed a forced-choice format (i.e., Better, Same, Worse, Don't Know) to compare the relative performance of the entire department in the current year

with that of the previous year. For each of these questions, an open-ended follow-up question was provided for respondents to comment, elaborate, or suggest methods for improvement. (See Appendix B for the actual questionnaire.)

The second survey instrument was completed by both the security department sample and the total management team sample. It was of assorted construction and employed a combination of forced-choice, open-ended, Likert scale and one-to-ten scale questions. More specifically, a five-point Likert scale approach was heavily utilized to measure fourteen specific traits and services provided by the department. Each scale formed a continuum from "Poor" to "Excellent." Two open-ended questions solicited input on other services which the department should be providing and general comments, suggestions, or criticisms. A number of forced-choice questions measured overall satisfaction with the services provided, comparisons with other hospital security departments, comparisons of the program in the current year versus the previous year, expectation levels of the program and feelings of safety at work. Depending on the particular question, the number of foils to select from varied. In addition, the overall performance of the department was measured on a scale of one-to-ten. (See Appendix C, for the actual questionnaire.)

The surveys were administered at three separate points in time, July 1983, June 1985, and June 1986. The first survey coincided with the onset of the study, the second

survey was administered approximately one year after the reorganization effort took place, and the third survey one year after that. (In effect, they represented a pretest-posttest-posttest measurement as will be discussed in the next section.) No survey was conducted in July of 1984 because that was the transition point for the reorganization of the program itself.

The surveys were administered at meetings conducted for all sample subjects. Attendance at security department meetings was mandatory, with absences only excusable due to sickness or vacation. Both surveys were administered at these meetings, but responses were voluntary and anonymous. Attendance at the total management meetings was not mandatory, but turnout and participation were expected to be high. (They routinely averaged between 50 - 70 percent.) Anonymity of these respondents was also maintained. Follow-up interdepartmental mailings were also done to provide an opportunity for people who missed these meetings to respond.

Both survey questionnaires had been "pretested" on five of the author's fellow department heads in the Human Resources Division of the hospital as well as the five original supervisors in the security department before the reorganization. This pretest was conducted in an attempt to make sure that the general instructions and questions themselves were understandable and that the questionnaires were easy and quick to complete. Some minor revisions were then made as deemed appropriate. In addition, the author

personally administered and scored the questionnaires by both sample groups. Instructions were provided, the forms were reviewed, and all respondents's questions were answered before the forms were actually filled out.

While the steps just described were designed to enhance the reliability of the survey instruments, no formal test was actually made to ascertain how reliable they were. This was not considered necessary, because the questionnaires were constructed in similar fashion to various other types of survey instruments, which have been widely accepted and used in social science research with success and reliability.

The biggest concerns over reliability did not deal so much with the instrumentation itself as with the sample subjects who were responding. Due to the largely negative view of the security department by the rest of the staff in 1983, there was a strong possibility of a negative "halo effect" which might have systematically biased the findings of the surveys. There was also some initial concern over how cooperative and truthful the security department members themselves would be at that time, because their own job security was at issue. These potential threats to reliability were more likely to influence results in the pretest applications and not so much during the posttest phases. However, there was little that could have been done to avoid them except to address them "diplomatically"

with the respondents when the general instructions were given for completing the questionnaires.

The reliability of the data collected from department records was also considered. In this context, reliability became a function of how well incidents or activities were initially reported, how well they were recorded and maintained for retrieval, and how accurately they were categorized. After the reorganization of the security program, these issues were well controlled. In fact, great care was taken to ensure that data was properly collected, recorded, summarized, categorized, and maintained. Accuracy and completeness were achieved in the following ways.

First, the hospital population was strongly encouraged to report <u>all</u> crimes, incidents, events, or suspicious circumstances. This was continually reinforced. Second, department members were specially trained on writing reports and documenting their activities. Refresher training was periodically provided and remedial training was also provided when problems with individuals were discovered. Third, all official reports written were assigned incident numbers, recorded in a running log, and maintained in a permanent file. These reports were reviewed daily by the shift supervisor and subsequently by the author or his assistant to ensure that they were complete, accurate, and categorized properly. Fourth, department members were required to document all their activities and account for

all their time on special daily activity forms which were turned in at the end of each shift for review by the shift supervisor. The data from each of these forms was summarized daily and compiled monthly along with all official report statistics.

All-in-all, the internally generated records-related data after the reorganization of the security program were considered reliable. Unfortunately, the same claim could not be made for the available data before the reorganization. First of all, department members were not previously trained in report writing nor required to document all their activities. This resulted in a lack of consistency in the way reports were written and categorized. It also prevented the generation of a large variety of data which could be used to compare with the reorganized program. Second, recordkeeping was sloppy at best. Much of what was written was "lost," and ongoing statistics were never maintained. Third, many crimes and other incidents were not reported to security personnel because of the general lack of confidence in them. Fourth, it was discovered that some reports made to security personnel were not even written up.

The author attempted to correct these problems during the year immediately preceding the reorganization, but was largely unsuccessful. As a result, department generated data before the reorganization was often incomplete and somewhat inaccurate, thereby seriously compromising reliability. To compensate as much as possible, all reports

on file were personally reviewed, corrected and reclassified to be consistent with the categorization scheme utilized for the reorganized program. A number of unreported incidents were also investigated and included in the data if they could be verified.

In the final analysis, the author contends that the "pretest" data presented in this study are as accurate as possible, but somewhat incomplete and probably under-reported. This in turn precluded certain "before and after" comparisons from being made and admittedly reduced the "actual versus observed" magnitude of many differences which might have otherwise been established in the analyses.

As a final note, a small portion of the data analyzed was not internally generated. This data included budgetary information which was produced by the Accounting Department, as well as certain crime statistics and census tract figures provided from the City of Detroit. This latter data was used to create per capita statistics for the immediate neighborhood surrounding the replacement facility and was compared to similarly generated data for the hospital itself.

RESEARCH DESIGN

From a methodological point of view, the ideal research design for this study, in terms of its survey-related component, would have been a truly experimental randomized control-group pretest-posttest design[81] or a randomized

Solomon four-group design.[82] Unfortunately, due to some specific limitations associated with this Action Research study, neither design was possible. Instead, the research design employed was the quasi-experimental one-group pretest-posttest design,[83] in spite of its minimal degree of control over various threats of internal and external validity.[84]

In general, only two relatively weak arguments could be made in defense of this design. First, it was an improvement over the historically prevalent one-shot case study (or posttest only) design.[85] Second, it reflected currently accepted (and popular) practice both in the areas of Action Research in general and program evaluations in particular. Neither reason, however, would be acceptable from a purely scientific point of view under ordinary and controllable circumstances.

Nevertheless, necessity dictated the use of such a design in this particular study because the conditions, under which the study had to be conducted, ruled out more sophisticated and desirable research designs. More specifically, random sampling was not employed for reasons already discussed. This alone would preclude the use of several potential research designs. Furthermore and perhaps more significantly, no relevant control group was possible because the entire population of interest (i.e., employees, physicians, patients, and visitors) was in fact, exposed to the independent variable (i.e., the new security program).

Hence, everyone would be in the experimental group and all designs requiring a control group had to be discounted.

These two major constraints virtually eliminated consideration of most of the more rigorous research designs which provide good control over threats to both internal and external validity.[86] The major remaining considerations, a counterbalanced design[87] and a one-group time-series design,[88] were also eliminated, because one of the conditions of the former (i.e., more than one variation of the experimental treatment) did not exist and multiple measurements associated with the latter could not be taken (for the same basic "political" reasons that a random sample was not approved by the hospital administration). The reader should note, however, that a set of second posttest measurements was incorporated into the design (reflecting a slight softening of Administration's reluctance to allow continual surveying of the program's potential effectiveness).

The limitations of a one-group pretest-posttest design received significant consideration and scrutiny. In the final analysis, however, the following assumptions were made to support the use of this option. First, the design would control for differential selection of sample subjects and experimental mortality should be minor (due only to turnover). Second, history and maturation should not be important factors due to the nature of the data being collected as well as the general context of the study

itself. Third, there should be little or no sensitization of results with respect to pretesting and posttesting, because the surveys would only elicit opinions and not accumulated knowledge. Fourth, there should be no recorded changes due to variations in instrumentation since the surveys should not have to be modified and the author would be administering and scoring all of them personally. Fifth, statistical regression should not be a major issue, because the sample subjects are not to be selected on the basis of any previous "extreme" scores. Sixth, interaction effects should be minimized because of the absence of control versus experimental groups. (However, this still must remain a concern at the level of the individual respondent.) As a final caveat, however, it is acknowledged that any violations of these assumptions might adversely affect the internal validity of the results obtained.

The external validity of the findings could also be challenged on a number of grounds. However, given the focus of the study, as a simple program evaluation and an example of Action Research, the generalizability of the results to other healthcare environments was not absolutely necessary to the main purposes of this study. Still, it is strongly advocated that replication studies be conducted on the general utility of the ACTION MODEL, upon which this endeavor was based.

The issue of research design, as it related to the departmental records component of the study, was less

salient and troublesome than for the survey component. For all practical purposes, the research design approximated a randomized control group pretest-posttest design as much as possible (the entire issue of randomization and sampling being largely irrelevant due to the source and nature of the data involved). The data obtained from the functional equivalent of a control group was provided from official Detroit Police crime statistics for the immediate neighborhood surrounding the site of the new hospital. To the degree that comparable statistics from D.P.D. records could not be obtained or were irrelevant, a basic pretest-posttest design was employed.

A brief word about the dependent and independent variables of the study would be in order at this point. A large number of dependent variables could have been identified with varying levels of importance. However, the major dependent variables of interest were:

1) Crime rates and their related statistics,

2) The variety, quality, and quantity of miscellaneous services provided by the reorganized program, and

3) The attitudes and perceptions of the hospital staff (including security personnel) towards the program.

The major independent variable, for purposes of this study, is the reorganized security program itself, as developed within the context of the theoretical framework presented in Chapter 3.

HYPOTHESES

In Chapter 1, ten research questions were provided as the functional equivalent of general hypotheses. In this section, they are restated in their original form as goal statements for the reorganized security program. Accompanying each goal is a varying number of objectives which if satisfied, result in the goal being attained.

It is data relating to each of these objectives which has been analyzed (as described in the next section). The accumulated results of those analyses form the basis for determining whether or not any given null hypothesis can be rejected and conversely, whether or not its alternative hypothesis can be accepted (i.e., determining that an individual goal has indeed been attained).

There are two separate sets of goals and objectives, one for the first year following the reorganization of the security program (1984 -85) and the other for the second year (1985 - 86). These allow for the equivalent of two posttests spaced a year apart. The goal statements are the same for both sets. (Hence, the hypotheses remain identical over both posttests.) Most of the objectives are comparable also. However, some differences and additions do occur in the second set of objectives, reflecting evolutionary changes in the direction and activities of the program over time.

The reader should note that the first four goals and their accompanying objectives in each set are the most

important ones. These are "strategic" or mission-related in nature. The remaining six goals and their accompanying objectives in each set are "supportive" or maintenance-related in nature. While the former focus on the services and ultimate results for which the reorganized program is responsible (i.e., its reason-to-be), the latter deal with developing and maintaining its resources, capabilities and potential at optimal levels.

1984 - 85

1) Prevention of security . . . related incidents which may result in personal harm, property loss, legal liability or disruption of routine health care operations.

   1.1) To reduce the number of crimes against persons below 1983 - 84 levels.

   1.2) To reduce the number of property crimes below 1983 - 84 levels.

   1.3) To reduce the amount of monetary losses associated with all crimes below 1983 - 84 levels.

   1.4) To establish a per capita crime rate which is lower than that for the surrounding community.

2) Minimization of the degree of harm, loss liability, or disruption associated with those incidents which cannot be prevented.

   2.1) To effectively control all occurrences of crimes still in progress once a response is made without additional injury to innocent persons or further avoidable monetary loss/property damage.

   2.2) To recover a larger percentage of stolen property (i.e., amounts) than during 1983 - 84.

2.3) To recover a larger percentage of stolen property (i.e., monetary value) than during 1983 - 84).

2.4) To apprehend a larger percentage of offenders committing crimes than during 1983 - 84.

3) Correction and/or elimination of the underlying problems which either cause or allow incidents to initially occur.

3.1) To investigatively solve a larger percentage of initially unsolved crimes than during 1983 - 84.

3.2) To investigatively identify all unsafe conditions and practices which contributed to the occurrence of crimes and to present specific, corrective recommendations for preventing their recurrences.

3.3) To ensure that all corrective recommendations for crimes . . . are fully implemented, once the appropriate approvals are received.

4) Provision of those miscellaneous services required for the general welfare and efficient operations.

4.1) To provide a broader range of miscellaneous "helping" services and general assistance to the institution than during 1983 - 84.

4.2) To provide in-service training to health center staff in the following areas:

Physical Management of "Disturbed" Persons
Fire Protection and Response
Tornado Protection and Response

4.3) To provide to health center staff the following loss prevention related services for personal use:

Vehicle Etching
Security, Safety and Fire Protection Pamphlets

4.4) To fully implement, administer and maintain the following loss prevention programs:

Access and Parking Control
Key Control
I.D. Badge
Vehicle Registration
Property Removal Pass
Operation I.D. of Health Center Property
Lost and Found

4.5) To provide active participation in the following community-wide crime prevention programs and activities associated with the Warren/Conner Coalition:

"Youth On Edge"
"Anticrime Task Force"
"Cops and Neighbors"
"Neighborhood Security Patrol"

4.6) To develop and implement a revised "New Employee Orientation" program on security . . .

4.7) To develop and implement a patient security program as part of the institution's patient education service.

5) The effective acquisition, development, and maintenance of all departmental resources.

5.1) To actively maintain at all times a manpower pool of qualified job applicants in each job classification.

5.2) To maintain "standing" manpower levels at all <u>times</u> which satisfy the institution's staffing needs.

5.3) To utilize a fair and effective selection process which includes job specific criteria, fingerprinting and police background checks, job reference checks, psychological assessment, structured interviews and employment testing.

5.4) To develop and utilize fair and effective promotional process which includes analysis of work records, structured interviews and assessment centers.

5.5) To provide active recruitment, selection and promotion of qualified applicants in accordance with all applicable civil rights legislation.

5.6) To maintain a racial and sexual composition of department members which reflects that of the community and the institution.

5.7) To develop and utilize a comprehensive department policy and procedure manual, which describes all job duties and expectations for all job classifications.

5.8) To conduct and continually revise an effective basic training program for all employees which consists of no less than 80 hours of classroom and O.J.T. instruction and also includes both written and practical application examinations.

5.9) To conduct and continually revise an effective advanced trained program for "sworn" employees which consists of no less than 130 hours of classroom and field instruction and also includes both written and practical application examination.

5.10) To provide additional job-specific training to all employees on an "as needed" basis.

5.11) To provide supervisory and management personnel with additional "professional development" training.

5.12) To maintain the institution's computerized security system in good working order at all times.

5.13) To maintain all department hardware and equipment in good working order at all times.

5.14) To maintain accurate up-to-date department records at all times.

6) The effective utilization and management of all existing departmental resources.

6.1) To maintain adequate shift coverage and duty assignments at all times, according to the institution's needs.

6.2) To identify changing institutional needs and provide both adequate resources and effective procedural responses to them.

6.3) To establish and maintain a "participative management" approach to routine decision-making involving employee input and advice.

6.4) To adhere to all applicable laws, policies, procedures, rules and regulations pertaining to the management and utilization of department resources at all times.

6.5) To assign, supervise, discipline, and reward personnel in a fair and equitable manner at all times.

6.6) To provide performance planning assistance to all personnel and to administer performance appraisals on an annual basis.

6.7) To satisfactorily pass all external and internal audits pertaining to department operations, effectiveness, and management.

6.8) To thoroughly investigate all complaints and concerns made about the department and take the appropriate remedial actions in a timely fashion.

7) Adherence to fiscal constraints on departmental resources in a cost-efficient manner.

7.1) To operate within approved budgetary allocations for the year.

7.2) To formulate and justify an annual budget request which is accurate and satisfies the department's actual fiscal needs without unnecessary expense to the institution.

7.3) To demonstrate cost-justification for <u>all</u> expenses incurred.

7.4) To generate at least $35,000.000 in parking revenue for the institution during the year.

8) A healthy organizational climate within the department which fosters positive working relationships and teamwork.

8.1) To improve department self-perceptions in terms of morale and performance over the previous recorded levels.

8.2) To reach consensus on department-related problems and their solutions via department-wide participation in the hospital's organizational climate survey.

8.3) To positively reward overall performance by matching performance ratings which merit salary increases in a fair and equitable manner.

8.4) To reward outstanding achievements through the development and successful implementation of a department "awards" program.

9) A positive image of the department within health center and community which promotes confidence, trust, cooperation, and favorable public relations.

9.1) To improve the institution's perceptions of the department in terms of its overall performance, image, and professionalism over previous recorded levels.

9.2) To reduce the institution's overall level of fear related to crime at the institution's new location.

9.3) To maintain positive working relationships at all times with other segments of the institution, patients, visitors, and physicians with whom contact is made.

9.4) To maintain positive working relationships at all times with local criminal justice, fire and community agencies/organizations with whom contact is made.

10) Effective communication links both within the department, and the health center.

10.1) To disseminate all information necessary for effective operations on a daily basis at shift briefings.

10.2) To provide complete, up-to-date and timely instructions on all new or revised policies, procedures, rules and regulations which pertain to department personnel.

10.3) To conduct periodic department-wide meetings for the purpose of joint planning, problem-solving and information sharing.

10.4) To conduct periodic "management team" meetings for the purpose of joint planning, problem-solving, information sharing and coordinating of routine operations.

10.5) To provide timely status reports to the appropriate authorities on department operations, individual incidents, emerging problems and alternative solutions.

10.6) To provide active participation on <u>all</u> assigned committees/task forces and at <u>all</u> relevant meetings conducted by the health center.

10.7) To disseminate security . . . information and instructions to all affected personnel in the institution whenever necessary.

<u>1985 - 86</u>

1) Prevention of security . . . related incidents which may result in personal harm, property loss, legal liability or disruption of routine health care operations.

1.1) To reduce the number of crimes against persons below 1984 - 85 levels.

1.2) To reduce the number of property crimes below 1984 - 85 levels.

1.3) To reduce the amount of monetary losses associated with all crimes below 1984 - 85 levels.

1.4) To establish a per capita crime rate which is lower than that for the surrounding community.

2) Minimization of the degree of harm, loss liability, or disruption associated with those incidents which cannot be prevented.

2.1) To effectively control <u>all</u> occurrences of crimes still in progress once a response is made without additional injury to innocent persons or further avoidable monetary loss/property damage.

2.2) To recover a larger percentage of stolen property (i.e., amounts) than during 1984 - 85.

2.3) To recover a larger percentage of stolen property (i.e., monetary value) than during 1984 - 85).

2.4) To apprehend a larger percentage of offenders committing crimes than during 1984 - 85.

3) Correction and/or elimination of the underlying problems which either cause or allow incidents to initially occur.

3.1) To investigatively solve a larger percentage of initially unsolved crimes than during 1984 - 85.

3.2) To investigatively identify <u>all</u> unsafe conditions and practices which contributed to the occurrence of crimes and to present specific, corrective recommendations for preventing their recurrences.

3.3) To ensure that <u>all</u> corrective recommendations for crimes . . . are fully implemented, once the appropriate approvals are received.

4) Provision of those miscellaneous services required for the general welfare and efficient operations.

4.1) To provide the same range and amount of miscellaneous "helping" services and general assistance to the institution than during 1984-85.

4.2) To provide in-service training to health center staff in the following areas:

Physical Management of "Disturbed" Persons
Fire Protection
Tornado Protection
Patient Relations
C.P.R.
Patient Searches

4.3) To provide to health center staff the following loss prevention services for personal use:

Operation I.D.
Vehicle Etching
Security, Safety and Fire Protection Pamphlets
Child Fingerprinting and Identification

4.4) To provide the surrounding community the following loss prevention services:

Child Protection Training
Child Fingerprinting and Identification
X-raying Halloween Candy

4.5) To administer and maintain the following loss prevention programs:

Access and Parking Control
Key Control
I.D. Badge
Vehicle Registration
Property Removal Pass
Operation I.D. of Health Center Property
Lost and Found
Patient/Visitor/Employee Search

4.6) To provide active participation in the following community-wide crime prevention programs and activities associated with Warren/Conner Coalition:

"Youth On Edge"
"Anticrime Task Force"
"Cops and Neighbors"
"Neighborhood Security Patrol"

4.7) To upgrade, revise, and implement the "New Employee Orientation" program on security . . .

4.8) To develop and implement a televised patient security program as part of the institution's patient education program.

4.9) To develop and provide a Security/Safety Fair for health center employees.

5) The effective acquisition, development, and maintenance of all departmental resources.

5.1) To maintain at all times a manpower pool of qualified job applicants in each job classification.

5.2) To maintain "standing" manpower levels at all times which satisfy the institution's routine staffing needs.

5.3) To hire qualified applicants on the basis of a fair and effective selection process.

5.4) To promote qualified employees on the basis of a fair and effective promotional process.

5.5) To provide active recruitment, selection and promotion of qualified applicants in accordance with all applicable civil rights legislation.

5.6) To maintain a racial and sexual composition of department members which reflects that of the community and the institution.

5.7) To review, revise, and utilize the department policy and procedure manual, which describes all job duties and expectations for all job classifications.

5.8) To review, revise, and conduct an effective basic training program for all employees which consists of no less than 80 hours of classroom and O.J.T. instruction and also includes both written and practical application examinations.

5.9) To review, revise, and conduct effective advanced trained program for "sworn" employees which consists of no less than 230 hours of formal classroom and field instruction and also includes both written and practical application examination.

5.10) To develop and conduct an annual maintenance training program for all employees, which consists of 80 hours of formal instruction for "sworn" personnel and 40 hours of nonsworn personnel.

5.11) To provide additional job-specific training for all employees on an "as needed" basis.

5.12) To develop, maintain, and utilize a video library of relevant training materials.

5.13) To develop and implement a "Field Training Officer" program for new employees.

5.14) To provide supervisory and management personnel with additional "professional development" training opportunities.

5.15) To provide interested personnel with additional training for the purpose of becoming in-house instructors.

5.16) To maintain the institution's computerized security system in good working order at all times.

5.17) To maintain all department issued hardware and equipment in good working order at all times.

5.18) To maintain accurate, up-to-date department records, including the incident reporting data base at all times.

6) The effective utilization and management of all existing departmental resources.

6.1) To maintain adequate shift coverage and duty assignments at all times, according to the institution's needs.

6.2) To identify changing institutional needs as they emerge and provide both adequate resources and effective procedural responses to them.

6.3) To adhere to all applicable laws, policies, procedures, rules and regulations pertaining to the management and utilization of department resources at all times.

6.4) To give time-off, assign, supervise, discipline and reward personnel in a fair and equitable manner at all times.

6.5) To provide performance planning assistance to all personnel and administer performance appraisals on a semi-annual basis.

6.6) To develop and utilize a managerial performance planning/appraisal system utilizing the M.B.O. approach.

6.7) To satisfactorily pass all external and internal audits/inspections pertaining to department operations, effectiveness, and management.

6.8) To thoroughly investigate all complaints and concerns made about the department and take appropriate remedial action in a timely fashion.

7) Adherence to fiscal constraints on departmental resources in a cost-efficient manner.

7.1) To operate within approved budgetary allocations for the year.

7.2) To formulate and justify an annual budget request for the upcoming year which is accurate and satisfies the department's actual fiscal needs without unnecessary expense to the institution.

7.3) To demonstrate cost-justification for <u>all</u> unanticipated expenses and overtime incurred.

7.4) To reduce turnover rates below the previous year's level.

7.5) To reduce absenteeism rates below the previous year's level.

7.6) To generate at least $35,000.000 in parking revenue for the institution during the year to partially offset department expenses.

7.7) To develop and market a training program for other institutions to utilize for a fee to partially offset department expenses.

8) A healthy organizational climate within the department which fosters positive working relationships and teamwork.

8.1) To maintain the department's favorable self-perceptions in terms of morale and performance at 1984 - 85 levels.

8.2) To reach consensus on department-related problems and their solutions via department-wide participation and collaboration in the Q.Q.R.H. process.

8.3) To positively reward overall performance by matching performance ratings which merit salary increases in a fair and equitable manner.

8.4) To reward outstanding individual achievements via a department "awards" program.

9) A positive image of the department within health center and community which promotes confidence, trust, cooperation, and favorable public relations.

9.1) To maintain the institution's favorable perception of the department in terms of its overall performance, image, and professionalism at 1984 - 85 levels.

9.2) To promote a general feeling of "personal safety" on the part of the institution's employee population.

9.3) To maintain positive working relationships with other segments of the institution, patients, visitors, and physicians with whom contact is made.

9.4) To maintain positive working relationships with local criminal justice, fire and community agencies/organizations with whom contact is made.

10) Effective communication links within the department, the health center, and the community.

10.1) To disseminate all information necessary for effective operations on a daily basis at shift briefings.

10.2) To provide complete, up-to-date and timely instructions on all new or revised policies, procedures, rules and regulations which pertain to department personnel.

10.3) To conduct periodic department-wide meetings for the purpose of joint planning, problem-solving and information sharing.

10.4) To conduct periodic "management team" meetings for the purpose of joint planning, problem-solving, information sharing and coordinating of routine operations.

10.5) To provide timely status reports to the appropriate authorities on department operations, individual incidents, emerging problems and alternative solutions.

10.6) To provide active participation on <u>all</u> assigned committees/task forces and at <u>all</u> relevant meetings conducted by the health center.

10.7) To disseminate security . . . information and instructions to all affected personnel in the institution whenever necessary.

10.8) To meet periodically and as needed with local criminal justice, fire and community agencies/ organizations for the purpose of maintaining positive working relationships, problem-solving and information sharing.

DATA ANALYSIS

Collected data was tabulated, coded, entered and stored in a personal computer using a software program designed for statistical analysis.

Data relating to official records was analyzed in the following ways. First, very little manipulation of the raw data needed to be made. Simple frequency tables were generated of all data collected over the three-year period of the study. They were compared where possible, as follows: Pretest vs. posttest 1, posttest 1 vs. posttest 2, and pretest vs. posttest 2. Where numbers were large enough, percentage changes were displayed. Due to the limitations discussed earlier about the availability of the collectible pretest data, pretest vs. posttest comparisons were more restricted than posttest 1 vs. posttest 2 comparisons. However, these latter comparisons were still useful in showing the ongoing development of the program over time. Figures comparing per capita crime rates within the institution versus within the surrounding community were generated as ratios of crimes per 1,000 people.

It is important to note that data generated from official records had to be interpreted in two ways. These figures reflected both "negative" indicators and "positive"

indicators. Negative indicators referred to such things as actual crime rates, monetary losses, turnover, and absenteeism. If the reorganized security program was successful, such figures should have decreased over time. Positive indicators referred to the miscellaneous services and activities performed by department members as well as arrests, values of recovered property, etc. They should have theoretically increased over time. Figures relating to racial and sexual composition of the department should have remained basically the same or increase in favor of minorities.

Analysis of the data generated from the survey questionnaires was handled as follows. For questions involving scales, basic summary statistics (e.g., means, standard deviations, etc.) were computed. Two-Tailed T-Tests of the differences between means were then conducted. A .05 = α level of significance was established to minimize Type I error.

Forced-choice questions were analyzed in terms of straightforward comparisons of percentages on frequency distributions. Open-ended questions were generally not figured into these analyses except where commonly reported issues, criticisms and/or recommendations were blatantly obvious and relevant. (Note: Such questions were originally intended for purposes of needs assessment and problem diagnosis and not program evaluation as such.)

All analyses made on survey data involved "within-group" posttest 1, and posttest 1 vs. posttest 2 comparisons for both sample groups. While visual comparisons between the security department's and total management team's scores were made, no formal "between-group" analyses were deemed necessary.

In order to properly evaluate the reorganized security program, the data collected had to be amenable to the techniques employed for analysis. Some of the statistical techniques used in this study were most appropriate for use on interval type data. However, due to the nature and quantity of the desired information, it was necessary to construct Likert scales in the questionnaires in such a way as to obtain ordinal type data. To use statistical techniques geared toward interval data on ordinal data would have been somewhat methodologically inappropriate, but it was still desirable to use the most powerful statistics possible. Therefore, the ordinal data were treated like interval data for purposes of this study. In defense of this decision, a quick look at other research from the field would show that there is ample precedent for this type of "bootlegging" and that acceptance of this practice is common.

At this point, the reader is reminded that the research hypotheses of this study were formulated on two sets of program goals and their accompanying objectives. Many of these objectives could be measured quantitatively and were

therefore amenable to the analytical techniques described above. Ultimately, the decision on whether or not these objectives had been achieved depended on the results of those statistical analyses. However, a number of the objectives were not readily quantifiable and therefore not as subject to objective evaluation. In these cases, subjective judgments were necessary. Such determinations were provided by the author's immediate supervisor, the Vice-President of Human Resources in consultation with other Vice-Presidents (as already discussed in the section on Sampling).

The program goals equated to research hypotheses, but only the operational objectives were actually subjected to analysis. Therefore, some functional reconciliation had to be made. In an ideal sense, every one of the objectives for any given goal would have had to be achieved in order for the goal itself to have been attained. However in reality, this would have been unlikely, especially given the fact that many of the objectives set forth for the reorganized program were considerably ambitious and could have become entirely dependent on external factors or constraints such as organizational "politics," reductions in program budget, etc. Therefore, a standard less than 100 percent achievement was deemed acceptable for purposes of the study.

To be sure, the overwhelming majority of objectives per goal should have been satisfied before that goal could be reasonably considered to have been attained. However, the

exact number or percentage was basically an arbitrary decision. No hard and fast standard would be appropriate "across the board," because the number of objectives per goal varies and they were not all qualitatively equivalent. As a rule-of-thumb though, a goal was considered to have been basically attained if no less than 75 percent of its accompanying objectives had been achieved (as determined by the analytical techniques described in this section). However, this guideline was subject to reconsideration in the event that a particularly important objective in one goal area had <u>not</u> been achieved even though 75 percent or more of the others had been (e.g., crimes against persons skyrocketed instead of decreased).

One final technique was employed in the analysis of this study. After all the objectives had been evaluated, an overall program rating was numerically expressed in the form of a percentage. While this figure was not directly relevant to the acceptance or rejection of specific hypotheses, it provided an overall benchmark score for comparing the program's success from year to year. The figure itself was reached by dividing the number of objectives which had been achieved by the total number of objectives listed. The objectives dealing with "Strategic" or mission-related goals were weighted with a numerical value of "two" (2) and those dealing with "Supportive" or maintenance-related goals had a value of "one" (1). The total possible value for all objectives was similarly

weighted. The result was a percentage (e.g., 85 percent or 90 percent) which can be interpreted as reflecting the program's overall effectiveness in accomplishing its goals and objectives. Note that this procedure was only relevant to the posttests. No comparable scoring scheme was possible for the pretest.

SUMMARY

In this chapter, an attempt has been made to show what methodological steps were taken in this study. This summary will briefly review those steps.

Two samples were surveyed. Neither had been randomly selected but rather were stratified due to "political" constraints imposed on the author by his supervisors. They included all security department members, and the entire management team of the hospital (i.e., administrators, department heads, in-house physicians, managers, supervisors, and head nurses). Both sample groups were surveyed once before the reorganization of the security program and twice afterwards. A third informal group, consisting of the author's supervisor and selected other administrators, factored into the study by providing independent evaluations of certain aspects.

Data collection was accomplished in a number of ways, the two major ones being a review of official records and the administration of two survey questionnaires to the sample groups described above. Examples of the types of

information, which was gleaned from official records, included criminal activities, security-related incidents, miscellaneous activities and services provided, economic losses and recoveries, budgetary expenditures, demographic profiles of department members, turnover and absenteeism rates, as well as crime statistics and census tract data for the surrounding neighborhood.

The survey instruments had been specifically developed for this study. One was administered only to the security department sample and the other was administered to both sample groups. These questionnaires had been designed to measure attitudes and opinions in a variety of areas, such as the morale, leadership, performance, and effectiveness of the security program. Measurement techniques included different types of scales (e.g., Likert), forced-choice questions and open-ended questions. They had been informally pretested and revised.

The ideal research design would have been a truly experimental randomized pretest-posttest control group design. However, for a number of reasons, not the least of which was the unavailability of a suitable control group, a quasi-experimental pretest-posttest experimental group-only design was employed with a second posttest measurement also being taken. Comparisons of certain crime statistics involved an approximation of a control group design with hospital per capita crime rates being compared to the surrounding community's per capita crime rates.

The research hypotheses took the form of goals and objectives for the reorganized security program. There were two different types of goals, those which were "Strategic" or mission-related and those which were "Supportive" or maintenance-related. For each goal there were several objectives which, in effect, constituted operational definitions of that goal. It was these individual objectives which were specifically evaluated.

Data analysis was aided by the use of a computer. Basic summary statistics were generated. Survey data were subjected to such statistical techniques as T-Tests. However, simple more-straightforward comparisons of records data were also made involving frequency tables and percentages of changes. Some findings were also reached through nonquantitative means involving personal observation and judgment. Overall program effectiveness ratings in the form of percentages were developed for both posttests.

Based on the analytical results, conclusions were drawn, and determinations were made on whether or not the goals had been attained (i.e., the functional equivalent of rejecting null hypotheses and accepting alternate hypotheses). These will be presented, along with appropriate recommendations and a discussion of the overall utility of the theoretical framework employed, in the final chapter of this study.

FOOTNOTES

[78]Stephen Isaac and William B. Michael, Handbook in Research and Evaluation, 2nd Ed., (San Diego: EDITS. Publishers, 1983), p. 55.

[79]Tony Tripodi, Phillip Fellin and Henry J. Meyer, The Assessment of Social Research, (Itasca, IL: F.E. Reacock Publishers, Inc., 1969), pg. 38.

[80]Tripodi, Fellin and Meyer, p. 41.

[81]Isaac and Michael, pp. 65-67.

[82]Isaac and Michael, pp. 68.

[83]Isaac and Michael, pp. 64.

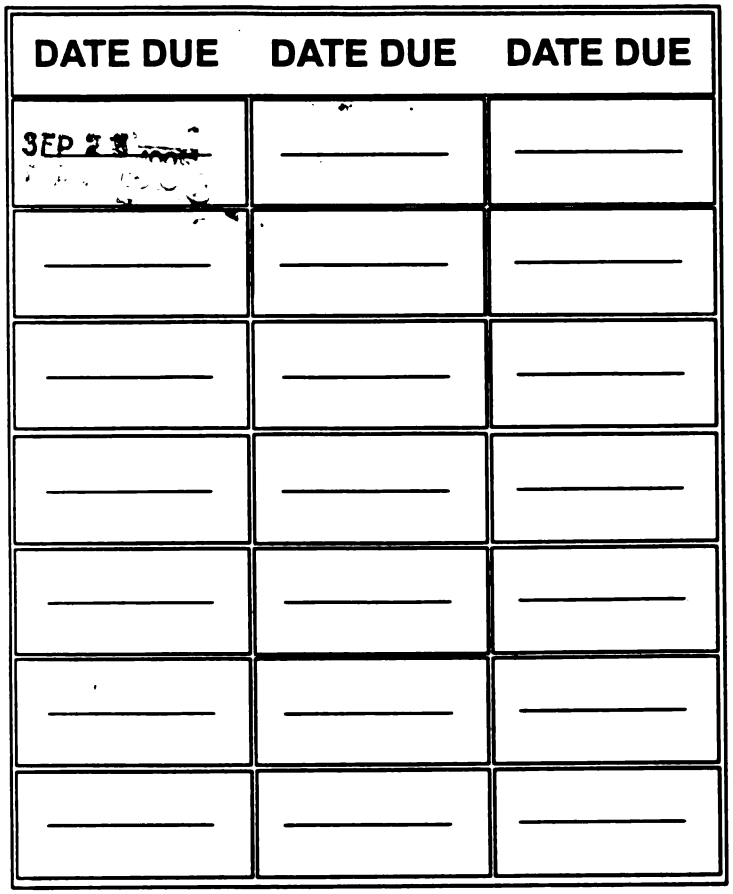
[84]Isaac and Michael, pp. 76.

[85]Isaac and Michael, pp. 63.

[86]Isaac and Michael, pp. 65-70, 73.

[87]Isaac and Michael, pp. 71-73.

[88]Isaac and Michael, pp. 73.



DATE DUE	DATE DUE	DATE DUE
SEP 2 [illegible]		

A PROGRAM EVALUATION OF SAMARITAN HEALTH CENTER'S DEPARTMENT OF PROTECTIVE SERVICES:

A NEW MODEL FOR PROVIDING PROTECTION IN HEALTH CARE ENVIRONMENTS

By

Robert Allen Smith

A DISSERTATION

Volume II

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

School of Criminal Justice

1989

CHAPTER 5

IMPLEMENTING THE PROGRAM

INTRODUCTION

In keeping with the overall theoretical framework presented in Chapter 3, an M.B.O. approach was employed in the initial evaluation, planning, and development of the security program. The Health Center administration's original mandate to reorganize the program became a simple mission statement for these activities. Five related goals and their accompanying objectives were then developed to address and identify needs, problems, and solutions in terms of security system components (i.e., People, Property, and Practices) at their various social system levels of analysis.

The goals and objectives themselves reflected discreet, comprehensive and mutually exclusive action statements. In effect, they constituted a basic performance plan (or blueprint) for developing the new security program within the context of the ACTION MODEL.

Goal #1 and its accompanying objectives related to: the process of Evaluating; the tasks of Assessing Needs and Diagnosing Problems; and the components Operations Audits, Physical Surveys, Opinion Surveys and Records Analyses. Goal #2 and its accompanying objectives addressed: the

process of Planning; the tasks of Establishing Direction, Setting Goals, Developing Strategies and Formulating Tactics; and the components Philosophy, Mission, Scope of Services, Goals, Objectives, Action Decisions, Performance Plans, Resource Plans, Sponsorship Plans and Implementation Plans. Goals #3 - 5 and their accompanying objectives dealt with the process of Executing and the task of Activating Plans. One goal and set of objectives pertained to People, one to Property and one to Practices (while all three components were addressed together in Goals #1 and 2).

Each one of the goals and objectives, described in this chapter, was successfully accomplished, thereby resulting in the reorganized security program which is the focus of this study. After each objective listed under Goal #1 is a summarized discussion of related needs and/or problems identified. After each objective listed under goal #2 is a summarized discussion of related recommendations and/or plans made. (Appendices are referred to as appropriate.) The objectives listed under goals #3 - 5 do not need further elaboration. However, they are followed by a section outlining what the reorganized program looked like, once developed and initially implemented.

MISSION:

Evaluation and subsequent reorganization of the Security program at Samaritan Health Center to meet the needs of the institution at its new location.

GOALS AND OBJECTIVES:

1) The identification of security-related needs and/or problems at the institution in terms of People, Practices, and Property.

   1.1) To identify the nature and extent of crime and security-related problems at the new location.

This was accomplished through a variety of methods. Several site and neighborhood inspections were made at all times of the day and night over a four-month period. Informal discussions were held with police officers who patrolled the area. Two formal interviews were conducted with the precinct commander who made two disconcerting announcements. First, due to their own recent staff reductions, the new hospital couldn't expect quick police response consistently. (Only one patrol vehicle routinely covered the area.) Second, the area was considered to be about the worst in the whole city. This sentiment was echoed by the crime prevention officer who staffed a mini-station across the street from the new location in a rundown public housing project. Both individuals felt strongly that the new hospital would have to provide the bulk of its own protection and could expect to encounter serious problems.

The crime prevention officer was also able to provide some hard statistics to confirm these concerns. In addition to crime statistics for the entire precinct, specific figures were compiled for the square mile within which the

new hospital would be located. Major crimes for the first nine months of the year (i.e., January - September 1983) were:

4	Murders (Homicide)
19	Rapes (C.S.C.)
74	Armed Robberies (R.A.)
31	Unarmed Robberies (R.N.A.)
102	Felonious Assaults (F.A.)
80	Assaults and Battery (A. & B.)
171	Burglaries (B. & E.)
147	Car Thefts (U.D.A.A.)
344	Thefts (Larceny)
208	Miscellaneous Other
1180	

With the exception of homicides all other reported crimes were considered to be gross under-estimates of the actual number which had occurred.

The construction site itself had been victimized repeatedly. In a six-month period (from April to September 1983) the construction company received reports from its contract security guard agency of several vandalisms, two burglaries, several thefts and even a felonious assault on an armed security officer, none of which were reported to the police (so weren't included in the statistics listed above). These crimes occurred in spite of 24-hour armed officer and guard dog coverage.

1.2) To identify the anticipated security-related demands for service at the new location.

Based on the somewhat startling findings described above, it became obvious that the health center would need to make a maximum effort in order to ensure a safe and secure environment. This would have to include a well-

staffed and equipped, professional security department, which could, in effect, duplicate the type and quality of services provided by the police. This in turn would require considerable training and the ability to adequately deal with extremely violent and life-threatening situations (i.e., the need for weapons). In addition, the potential liability problems, associated with private citizens committing misdemeanor arrests (as discussed in Chapter 1), would suggest a need to obtain increased legal authority for the health center's security personnel.

Beyond the obviously acute need to be able to provide comprehensive protection against both personal and property crime, other general needs had to be considered. To a large degree the author relied on his own experience, as well as the opinion of respected colleagues in the field, to identify a broad spectrum of security-related services, which should theoretically be provided by any hospital security department (not to mention safety, disaster and fire-related services which aren't really the focus of this study). These do not require elaboration here but are generally included in the Scope of Services Statement contained in the Appendices. They are also reflected throughout the Goals and Objectives of the reorganized program.

It was also deemed important to address any other services which were expected and/or desired by the rest of the institution. To identify such specific needs and

wants, the employee population itself was queried. From August until December 1983, interviews were conducted with all administrators and department heads, as well as many selected managers, supervisors, physicians, and hourly employees. These interviews covered a broad range of topics but included questions relating to specific types of services that the respondents felt their own security department should provide (or provide better). Similar discussions were conducted with the incumbent security personnel themselves. Furthermore, formal questionnaires were administered at a total management meeting in August, 1983. (The interviews were actually follow-ups to these questionnaires.)

The questionnaires were the same as appears in Appendix C. However, they also included a variety of additional multipurpose questions relating to the impending move, desired services, and the need for arrest powers. Since the questions relating to desired services were basically open-ended and exploratory, "hard" statistics were not maintained (also because few actual suggestions were made). However on the forced-choice question relating to the need for arrest powers, 71 percent of the respondents indicated "Yes" while another 12 percent had "No Opinion."

In the final analysis, the input from the health center staff yielded few demands for service which had not already been addressed by the author. However, the very process of asking served two other purposes. In many cases, the

results showed support for the author's own views (particularly important on the arrest powers issue). It also reassured many people that positive steps were being taken on their behalf.

One recurring theme was noted throughout the interview process. There was a consistent desire to have a public-relations oriented security department, which would be sensitive to the emotional and interpersonal complexities of a health care environment.

1.3) To identify the capabilities and limitations of incumbent department personnel in terms of general qualifications, knowledge, skills and abilities necessary to meet anticipated demands for service.

As it became increasingly clear what the anticipated needs would be at the new location, attention focused on the existing security department's ability to meet them. This involved both the department's performance as a whole and the characteristics of the individuals in it.

An assessment of overall performance was made by the author's personal observation and participation, as well as analysis of the total management questionnaires already discussed. Within one month of serving as Director of the department, the author agreed with the view described to him by administration upon initial employment: namely, the security program was in shambles. Discipline was almost non-existent. The quality of services rendered was poor and many services, ordinarily provided by a hospital security department, weren't even attempted. Leadership was

questionable at best; morale was low; and little was ever accomplished.

These observations were largely confirmed by the department and management staff alike. For example, in the surveys administered in August 1983, twelve separate categories relating to department performance were assessed on Likert scales, with numerical values from 1 to 5 (i.e., "Poor" to "Excellent"). There were 14 respondents from the security department and 105 respondents from the total management team. The results are shown in Table 5.1.

TABLE 5.1
OVERALL PERCEPTIONS

	Security Dept.			Management Team		
	n	$\bar{x}$	s	n	$\bar{x}$	s
Public Relations	10	2.80	1.03	101	2.39	.77
Crime Prevention	10	2.40	.97	90	2.13	.69
Investigative Skills	10	2.30	1.06	85	2.08	.71
Crisis Intervention	9	2.56	.89	86	2.24	.83
Communication Skills	9	2.44	1.01	99	2.24	.77
Job Knowledge	9	2.44	1.01	88	2.33	.74
Dedication/Interest	10	2.30	1.25	92	2.39	.86
Professional Demeanor	9	2.33	.87	92	2.03	.76
Response Time	9	3.56	1.13	88	2.69	.91
Miscellaneous Services	10	2.70	.95	87	2.71	.81
Overall Image	10	2.70	.82	96	2.23	.80
Overall Performance	10	2.80	.79	96	2.28	.71

$\bar{x}$		INTERPRETATION
0.0 to 1.49	=	Poor
1.5 to 2.49	=	Needs Improvement
2.5 to 3.49	=	Adequate
3.5 to 4.49	=	Good
4.5 to 5.0	=	Excellent

Neither group rated the department very favorably in any category. As might be expected the security respondents

tended to rate themselves slightly higher than the total management team did. However on only one-half of the categories did they even rate themselves as "Adequate." On the rest they indicated a "Needs Improvement" rating. The total management team respondents were considerably less generous. They rated the department as "Adequate" in only two categories, Response Time and Miscellaneous Services. In all other categories, they felt that the department only merited a "Needs Improvement" rating. Their numerical mean scores were generally lower also.

Based on both observation and survey results, it became quite clear that the department as a whole was not even capable of adequately protecting the two existing facilities, which were located in comparatively safe locations (for the City of Detroit). There was no question that it could not satisfy the demands for service at the new location. However, to rule out the possibility that the deficiencies were not merely a function of poor leadership, training, and/or motivation, the characteristics of the incumbents themselves were also analyzed.

There were 47 F.T.E.s (Full Time Equivalents) at the two existing facilities, but 11 of those were poorly paid contract security guards, who often rotated to the health center from other assignments. Few were permanently assigned and their overall turnover rate was over 100 percent per year. They were also not under the direct control of the health center and did not feel any direct

loyalty to it. This contingent could obviously not satisfy the anticipated needs at the new location.

The 36 "in-house" department members generally did not fare much better. Absenteeism and tardiness were rampant. Discipline was high, even though the former Director was known to be very permissive and to overlook most infractions. Training was non-existent. One-third of the department didn't even have a high school diploma (or equivalent). One officer actually attended through only fourth grade. Many were "advanced" in years. A large percentage had a number of miscellaneous "problems" which were not conducive to good security employment standards. (In addition, subsequent psychological testing in later months revealed several officers with developmental disabilities, personality disorders, and/or low IQs.) Below is listed a more detailed breakdown.

FACTOR	STATUS
Education:	College Degree 0% Some College 12% H.S.D. or G.E.D. 56% Less than H.S.D. 32%
Training:	Virtually no documented inservice training within the last two years. No preservice training program existed for all. Only 10 officers ever received any formal training at all (in any job).
Age:	Average age was 46 years old 1 officer was 82 years old 4 officers were over 60 years old 15 officers were over 43 years old
Absenteeism:	Annualized average of 10 sick-days per officer.
Tardiness:	Annualized average of 14 tardies per officer.

Other Unpaid Time-Off:	Annualized average of 6 unpaid days per officer (i.e., after all paid time is used up).
Discipline: (Oct. 82 - July 83)	3 officers who have received at least one written reprimand. 4 other officers who were also suspended (3 more than once). 6 other officers who had ultimately been discharged. A total of 13 officers (38% of department) who have received disciplinary action. A total of 9 written reprimands and 15 suspensions.
Miscellaneous:	8 officers with health/physical problems which interfere with job performance. 4 officers with demonstrated violent tendencies. 1 officer who was basically illiterate. 3 officers who were transferred into Security after problems in other departments. 3 officers who were hired into department after being fired by contract agency used by the hospital. 3 officers who were known to carry illegal weapons. 8 officers who currently had warrants for their arrest. 5 officers who had conviction records.

While many of these undesirable factors could be attributed to poor management and direction, some could not. Remedial action (e.g., training or sound leadership) could not adequately upgrade the capabilities of all of the department personnel to envisioned levels necessary for the new location. In effect, many of the people were simply not qualified for the upcoming task.

1.4) To identify the capabilities and limitations of current staffing levels, organizational structure, and functional duties of the department to meet anticipated demands for service.

Given the existing post and patrol assignments, the staffing levels were grossly inadequate to ensure consistent

coverage at all times when needed (i.e., approximately 6 F.T.E.s short). There was no replacement coverage factored into the staffing levels for lunches, breaks, sick days, holidays, vacations, etc. As a result, posts and patrols often went uncovered. This problem was compounded by the fact that routine weekly schedules allowed one-half the staff to have each weekend off, thereby building in shortages which could have been avoided by spacing out days off more effectively (e.g., every third weekend off). While it was clearly understood that different staffing levels would probably be needed at the new location, it was important to make sure that the same mistakes weren't going to be made.

The department was organized around a Director, four Supervisors, a part-time Clerk Typist, and two levels of Officers. Promotion from the lower Officer level to the higher one was more on the basis of seniority than objective selection criteria. Furthermore, lateral entry to the higher Officer position or Supervisor was not possible. Even well-qualified job applicants had to start at the entry level Officer position.

At one facility, each shift had its own Supervisor. Officers were accountable only to their own Supervisor, and not another one. In his absence, an officer was placed "in charge," but he had no formal authority nor responsibility other than to make duty assignments. In fact, he could assign himself to a post and not even oversee the operations

of the other members of his shift. At the other facility, there was only one day-shift Supervisor who was not expected to provide any direct supervision of the other two shifts, nor even work weekends. He was allowed to operate independently from the Director who spent most of his time at the larger facility. In fact, both facilities operated autonomously from each other and were a single security department primarily in name only. Needless to say, these structural arrangements could not continue at the new location.

The functional duties of the department were, for the most part, not formally defined, delineated, nor enforced (unless a complaint was lodged). Job descriptions were out of date and did not adequately summarize the routine responsibilities of the positions. (Some members had never even seen their job description.) The overall role of the department was not clearly understood by many members. In fact, there were no formal goals, mission, nor scope of services. There was little consistency on how specific duties were to be performed and, in some cases, what those duties even were for any given post or patrol. For example, the floor patrol had no specific duties except on one shift. Several officers had their own preferred duty assignment and didn't know what to do if assigned elsewhere. Contract guards were at a greater disadvantage. They were routinely given only a brief orientation before being assigned and often received minimal supervision.

In the final analysis, the department was in considerable disarray in terms of its staffing, organization, and functions.

1.5) To identify personal equipment needs for department personnel at the new location.

The existing security department had very little in the way of personal equipment other than traditional security uniforms (which were not consistently worn anyway) and radios (which were several years old and in constant need of repair). Given the level of sophistication of the program not much else was needed. However, specific equipment needs were identified for the new location.

A completely new radio system would be needed to replace the aging one. New uniforms, which did not reinforce the existing stereotype of "guards" but rather would convey a more positive image, were deemed necessary. Since the site of the new hospital would include numerous parking lots spread out over a large area, effective patrol could only be accomplished with well-equipped vehicles. They would facilitate timely coverage, quick response, convenient escort service, and also a measure of protection for the security personnel themselves. Contingent upon approval for arrest authority and weapons, a variety of typically police-related items would be required. These included the firearms themselves, holsters and belts, ammunition, nightsticks, handcuffs, badges, etc. In addition a number of additional but routine pieces of

equipment, which were not readily available to the existing department, were needed. These included such things as keys (the current personnel were not entrusted with keys to sensitive areas), flashlights, raincoats, jumper cables, etc.

1.6) To identify potential physical security hazards and needs at the new location.

This process had actually begun when the author was originally retained as a consultant for the health center. It involved site inspections, meetings with planners, architects and contractors, as well as reviews of site plans and blueprints. The main concerns were inadequate lighting, ease of accessibility to parking areas and buildings, unrestricted traffic-flow patterns, and potential hiding places or blind spots. In addition, the potential hazards of the surrounding neighborhood were taken into consideration (e.g., abandoned buildings close by).

Since this process began in the planning and design stages of the new facility, there weren't many existing problems to be corrected, but rather mostly anticipated ones to be avoided (a more practical and logistically feasible task). In this regard ten "zones" of potential vulnerability were established. Within each, zone specific types of hazards were anticipated. Corresponding countermeasures were then developed. (In Appendix D there are provided site plans and an outline describing the zones and the security products deemed appropriate for each one.)

1.7) To identify institution-wide deficiencies and needs in terms of operational policies, procedures and practices which relate to security.

A review was made of the health center's administrative, operational and human resources policies and procedures, as well as the institution's disciplinary rules and regulations. Discussions were also held with relevant administrators, department heads, and personnel specialists. As a result, it was discovered that the issue of security was not even addressed formally by the institution. With the exception of disciplinary rules pertaining to theft and unauthorized weapons, there were no institution-wide policies, procedures nor even accepted practices relating to security. Any efforts in this regard would have to be made from scratch.

1.8) To identify departmental deficiencies and needs in terms of operational policies and procedures and administrative rules and regulations.

Discussions were held with department Supervisors, and a review of departmental records was made. The latter process was particularly problematic, because record-keeping was poor. Attendance records, personnel files, correspondence and other administrative records were not properly organized, filed nor even kept updated. Many records were simply missing. No single department standard-operating-procedure (S.O.P.) manual existed. Furthermore, the records for each facility were not centralized. In fact, it

took nearly a week to even compile and sort out the materials which were available.

It was discovered that there were basically no written administrative rules and regulations, with only a couple of exceptions and these had not been reviewed or updated in years. Most of what existed was word-of-mouth. Routine operating procedures for posts and patrols were incomplete, not current, nor readily available to all members of the department. Some were even irrelevant to actual practice. Whenever a change in procedure was made in writing, it was posted in the squad rooms for a few days and then tended to disappear. There was seldom a formal announcement, because shift briefings did not occur and department meetings were rare. Other than a fire response plan, there were no specific emergency procedures to follow.

In summary, there was virtually nothing which could be applicable to administration or operations at the new location. Everything would have to be formulated independently.

2) The development of a comprehensive reorganization plan which satisfies the identified security-related needs and/or problems at the new location in terms of People, Property and Practices.

   2.1) To develop a formalized Philosophy, Mission, Scope of Services, and Set of Goals/Objectives for the department which are compatible with identified demands for service.

These statements were developed as a blueprint for the reorganization effort. All of them, except the Objectives, were submitted to administration and approved. The objectives were approved by the author's Supervisor. (In Appendix E the Philosophy, Mission, Scope of Services, and Goal statements are contained.) The Objectives may be found as testable hypotheses in Chapter 4.)

2.2) To revise the staffing levels, organizational structure and functional duties of the department in accordance with identified capabilities/limitations and demands for service.

Since the existing staffing, organization, and duties were determined to be inadequate for even current conditions, they were obviously not appropriate for attempting to satisfy the anticipated and more acute needs and demands for service at the new location. Therefore they were largely discarded from further consideration. Instead, a completely new department "form and function" was developed.

New job classifications were developed. They included:

Manager
Supervisors
Specialists
Officers
Dispatchers

New sets of general duties and responsibilities were clearly formulated for each classification. Specific post, patrol, and zone (i.e., a combination of a post and patrol) assignments were made for these classifications in accordance with anticipated needs at the new location.

Reporting relationships and chain-of-command were clearly defined.

Staffing levels by classification and number of post, patrol, and zone assignments were established for each shift and day of the week. These reflected the needs for both routine coverage and consistent relief/replacement coverage. (A master schedule was then created to ensure that such coverage would be maintained 24 hours a day, 7 days a week.)

Since the health center was moving into a single facility from two separate ones, the needed staffing levels could be reduced. For example, there would be only one emergency room to staff instead of two. Also the use of electronics (e.g., card readers, alarms and cameras at employee entrances) would eliminate the need for a person at some posts. Therefore the total number of F.T.E.s was able to be reduced to 40, while still affording better coverage than before.

In Appendix F a simplified organizational chart of the reorganized department, with accompanying staffing levels for each job classification, is contained. Also provided is a manpower planning flow chart and work sheet, which the author developed for use with the ACTION MODEL and utilized in determining the appropriate staffing levels.

2.3) To develop and/or revise operational policies/procedures and administrative rules/regulations of the department in accordance with identified deficiencies and needs.

Due to the fact that the existing policies/procedures and rules/regulations of the department were wholly inadequate, a completely new set had to be developed. In this regard, standard operating procedures were created for each classification and corresponding post, patrol, and zone assignment according to shift and day of the week. Administrative rules and regulations were also promulgated to cover every possible contingency and eliminate uncertainty by staff members. Everything was formatted as follows (where appropriate):

- Policy (i.e., the general department position on a particular issue)
- Scope (i.e., the people subject to the policy)
- Objective (i.e., the purpose or reason for the policy)
- Procedure (i.e., the steps to follow in compliance with the policy)

When completed everything was compiled into a single department manual, which was given to each employee and updated as necessary. The manual was organized into the following sections:

- General Orientation
- Department Organization
- Administrative Rules and Regulations
- Routine Operational Procedures
- Special Procedures
- Legal Procedures
- Emergency Procedures
- Miscellaneous

A complete Table of Contents covering all topic areas is presented in Appendix G.

2.4) To develop specific, job-related qualifications and employment standards for department personnel which can satisfy the identified demands for service.

Once a determination had been made on the kinds of tasks (i.e., duties and procedures) which would have to be performed in satisfying anticipated needs and demands for service, it was necessary to determine what kinds of people could best carry them out. For each job classification, basic requirements were established. These standards were considerably higher than had been expected for the existing department, but were not made to automatically exclude incumbents.

Since there was intent to have arrest powers, certain minimum requirements established by the Michigan State Police Private Security Section (which would license such authority) were established as minimums. These included such basic requirements as a high school diploma or equivalent and no felony convictions within five years for any member of the department. Beyond that, higher standards were established for all Managers, Specialists, and Supervisors who would receive arrest authority. Varying experience and education levels were established for different classifications and responsibilities. Driving records and the ability to obtain a concealed weapons permit were also factored in. Certain health standards were established also.

All the set qualifications and standards were developed to be job-related, necessary, and nondiscriminatory. Minimum entrance requirements from a number of security organizations and police departments were reviewed first. The personnel department and Vice-President of Human Resources contributed to the effort. (Examples of all the Job Descriptions which were ultimately developed are contained in Appendix H.) They include both the minimum entrance requirements and the routine duties and responsibilities associated with each new classification.)

2.5) To develop selection procedures which identify the most qualified job applicants in accordance with applicable civil rights legislation.

A comprehensive selection process was developed. Both the methods and criteria were closely scrutinized so as to be able to screen for the best candidates without adversely impacting on protected classes. All relevant federal and state laws were considered, as were the health center's employment policies. The process included:

- Completed applications and resumes
- Interviews which were structured and scored
- Written "scenario" tests which were scored
- Commercial honesty-personality tests
- Background checks (employment, criminal records, driving records, references, etc.)
- Physicals (including drug screens)
- Psychological assessments (by a police psychologist who administered a battery of tests and interviewed applicants)

The selection process was reviewed by the health center's civil rights attorneys (along with the actual employment standards themselves). The commercial test was reviewed by the Director of the Michigan Civil Rights Commission. Even the police psychologist's personal "track record" and references were checked.

2.6) To develop employment incentives which attract, reward and retain qualified job applicants.

The employment standards and selection process were designed to create a professional security staff, which would be on a par with a good police department. However, the existing compensation and benefits levels were not sufficient to attract nor retain the calibre of personnel desired. In fact, they weren't even competitive with most other hospital security programs in the area. Therefore, wage scales and benefit packages were reviewed and revised.

Wage and salary surveys were conducted of the local hospitals with the most prestigious security departments, as well as some of the metropolitan police departments. Compensation specialists conducted job evaluations of each classification. New wage scales were then developed. The Manager, Specialist and Supervisor classifications were made "exempt" level status and as such were eligible for the best benefit package available in the health center. Furthermore, all classifications were made eligible for annual merit increases based on performance, so that good

employees would receive appropriate economic rewards. Longevity increases were eliminated.

The resulting increases in cost for salaries and benefits would have ordinarily been prohibitive to the institution. However, since staffing levels could be reduced at the new location, the proposed increases would have been more than offset by the savings in staff reductions. The result would be the best compensated hospital security department in the state, which could also compete with many public police departments.

2.7) To develop a comprehensive preservice training program which provides the basic knowledge, skills and abilities necessary to satisfy the identified demands for service on department personnel.

Even with well-qualified employees, it was necessary to provide some type of training which addressed the specific needs of the health center, as well as sound security and law enforcement techniques. Formal police academy training would be too long, expensive and, in many cases, largely irrelevant to a health care environment. No suitable private security training resource was in existence. Hence, it was necessary to develop the department's own training program.

In order to qualify for arrest authority, the Michigan State Police required a minimum of 145 hours of specified training. (It dictated the topic areas and corresponding objectives, but did not actually provide the training itself.) The State Police requirement constituted a minimum

curriculum around which additional training was also developed. Part of this training was institution-specific, covering the entire department manual. The remainder dealt with general security, hospital security, safety, fire, disaster, and human-relations related topic areas. Even some of the State Police requirements were expanded, based on the author's previous personal experience with a security organization granted arrest authority employing the State Police training requirements.

The actual training topics (other than State Police and department-specific) were selected after a review of all available security and law enforcement training materials. A previous hospital training program (of 200 hours) developed by the author was also heavily utilized. Learning objectives for each topic area were also derived in part from the reviews. For some topic areas complete lesson plans were developed. For some (e.g., legal issues) outside instructors (e.g., lawyers) were employed to develop them and ultimately instruct in those areas. A variety of related training aids and reference materials were compiled. Finally, test questions and practical application exercises were created, based on the learning objectives.

The original training program consisted of 240 hours of instruction. Over the entire period of study, it would be continually original and upgraded to 360 hours. (A topic outline of the original version of the program is contained in Appendix I.)

2.8) To develop specifications and performance requirements for products which satisfy the personal equipment needs of department personnel.

This was accomplished primarily by reviewing product literature, consulting with professional colleagues, and relying on personal experience. Most personal equipment needs and specifications were easy to determine. Radios, firearms, and vehicles required considerably more effort. For these, formal requests-for-quote (R.F.Q.) were developed to eventually be sent to vendors. These documents specified required amounts, performance capabilities, desired features and durability needs. Warranties and service arrangements were also considerations.

2.9) To develop specifications and performance requirements for products which eliminate identified physical hazards and satisfy identified needs.

Performance capabilities for major security hardware items (e.g., C.C.T.V., card access systems, etc.) were addressed much in the same way as for personal equipment, only on a grander scale. Seminars on physical security systems were also attended to keep abreast of the state-of-the-art. Detailed R.F.Q.s were eventually developed.

2.10) To develop comprehensive institution-wide security-related programs, policies, procedures and practices which satisfy identified deficiencies and needs.

A wide variety of improvements were needed at the new location to supplement the new security department itself. After considerable effort and collaboration with various managers, department heads, and administrators, a number of

hospital-wide programs, policies and procedures were formulated for approval and subsequent implementation as the move took place. They included:

- Designated parking and employee entrance assignments (based on shift and work area location in the hospital)
- Picture I.D. badges (which could be used in card readers at parking lots and employee entrances)
- Key distribution and control (on a need-to-possess basis)
- Property "check-out" procedure (for ensuring that health center property was returned upon termination of employment)
- Search procedures (i.e., staff, visitor and patient)
- Property pass and removal authorization (for leaving the premises with health center property)
- Vehicle registration (with numbered stickers for identification purposes)
- Visitor control (i.e., hours, conditions, and passes)
- Vehicle towing (for removing improperly parked vehicles)
- Lost and found
- Handling patient valuables

In addition, a number of disciplinary rules and regulations were incorporated to support the program. Examples were:

- Failing to adhere to health, safety, and sanitation rules and practices
- Failing to wear an I.D. badge
- Failing to comply with parking regulations

- Theft or misappropriation of property belonging to the health center, employees, visitors or patients
- Possession of unauthorized weapons (as defined by the security department)
- Participating in any criminal act during working hours
- Interfering with or refusing to cooperate with security personnel in the performance of their duties

Institutional legitimation was also sought for the new security program. A formal document supporting the proposed reorganization and giving it authority was developed for administrative approval and sanction. (See Appendix J.) Finally, security-related issues were written into the health center's employee handbook; and a presentation was developed for new employee orientation.

2.11) To budget all reorganization plans and proposals within fiscal capabilities and constraints.

All reorganization efforts were made with cost considerations in mind. The construction budget for the new facility contained funds for unspecified security hardware. The recommendations, which were ultimately made, exceeded these funds, but it was possible to show that the cost savings in personnel (i.e., over 3 F.T.E.s could be eliminated by installing certain hardware) would offset these overruns in less than three years.

The entire security program was formulated in light of a zero-based budgeting approach which attempted to cost-justify every component. (The sample Z.B.B. work sheets,

which were created and used in developing the proposed budget, are contained in Appendix K.) There was a previous administrative mandate that the new security program (in whatever form it might take) could not exceed the costs of the existing one. Fortunately, due to the staff reductions planned, the proposed annual operating budget was actually slightly less than the approved budget for the previous year. Hence, fiscal considerations would not be a major factor in obtaining approval for the reorganization.

2.12) To obtain both formal approval of and informal support for all reorganization plans and proposals.

This was by far the most difficult and complicated task associated with the reorganization effort. While the general climate at the health center as receptive to change, two specific recommendations were quite controversial. More specifically, the proposals for arrest authority and firearms were difficult for many to accept, especially in a religious institution which had nuns as department heads, administrators, and members of the board of directors. Furthermore, the possibility that some of the existing security personnel might be displaced (i.e., laid off) was not particularly welcomed, because in spite of their shortcomings, they were still considered part of the hospital "family."

Individual "sponsors" on the administrative staff were sought out. Every possible source of resistance (from hourly employees to the board of directors) was anticipated

and analyzed. Appropriate strategies were then developed to neutralize resistance and garner support. No simple strategy was possible. Different components of the overall proposal required different strategies, as did different people whose approval was necessary. In fact, in some cases, the change strategies had to be modified over time for the same target populations. In general, however, a "facilitative" strategy was most appropriate for the majority of the administrative staff, a "re-educative strategy" for the department heads and total management team (i.e., managers and supervisors) and a "persuasive" strategy for the general employee population. Ultimately, a "power" strategy was even necessary for some security department personnel, who openly opposed the reorganization. In all cases, there were exceptions to these approaches.

At a formal level, the proposed reorganization had to receive approval first from the author's supervisor, then the entire administrative staff, and finally, the board of directors. The corporate risk managers and legal staff also required approval. Informally, support was necessary from the department heads, the medical staff, the total management team, nursing in particular, and the hourly employees in general. The Detroit Police Department also had to give support for the arrest authority and firearms components. Finally, the Michigan State Police had to approve the overall program. Each of these groups were approached with both formal and informal presentations.

In spite of all the efforts taken, approval and support was not unanimous. Many people were skeptical that the proposals would be appropriate and/or successful. The board of directors was especially concerned about the impact of an armed "police" department on minorities. The existing security department was concerned about its own survival. Nevertheless, in the final analysis, there was a general consensus to approve and support the proposals made. Work began immediately to implement those proposals as described in the following three Goals and their accompanying Objectives.

A formal reorganization document was prepared and presented to the administrative staff, board of directors, and corporate officials. It provided all the details of the proposed reorganization as well as appropriate justification. It was over 60 pages long and had an executive summary. (Its table of contents is provided in Appendix L.)

3) The acquisition and preservice preparation of qualified security personnel.

   3.1) To place into effect the developed employee incentives for department personnel.

   3.2) To develop a qualified applicant pool for both internal and external candidates.

   3.3) To screen, select, and employ the most qualified applicants in accordance with identified staffing needs and the job-related qualifications, employment standards, and selection procedures which have been developed.

3.4) To orient all department employees to the institution and the department's Philosophy, Mission, Scope of Services, and Goals/Objectives, organizational structure, functional relationships, and administrative rules and regulations.

3.5) To train all department employees in accordance with previously developed preservice training program.

4) The dissemination and implementation of effective security-related practices.

4.1) To place into effect the revised staffing levels, organizational structure, functional relationships, and administrative rules/regulations of the department.

4.2) To train all department employees on the revised operational policies/procedures of the department.

4.3) To orient the rest of the institution on the capabilities, services, and operational procedures of the reorganized security department.

4.4) To place into effect the revised operational policies/procedures of the department and commence routine operations at the new location upon its opening.

4.5) To publicize within the institution all previously developed security-related programs, policies, procedures, and practices as well as provide relevant training to all affected employees, as necessary.

4.6) To place into effect all previously developed security-related programs, policies, procedures, and practices at the new location upon its opening.

5) The acquisition and operationalization of security-related property.

5.1) To develop a qualified vendor pool for the purchase of personal equipment to be used by department personnel.

5.2) To screen and select vendors and purchase specific types of equipment in accordance with developed specifications and performance requirements.

5.3) To ensure the delivery, proper installation, and successful operation of all purchased equipment.

5.4) To assign and issue specific equipment to department personnel on a need-to-possess basis.

5.5) To develop a qualified vendor pool for the purchase of products which minimize identified physical hazards and satisfy identified needs.

5.6) To screen and select vendors and purchase specific types of products in accordance with developed specifications and performance requirements.

5.7) To ensure the delivery, proper installation, and successful operation of all purchased products.

5.8) To assign and issue specific products to institutional personnel (i.e., nonsecurity) on a need-to-possess basis.

5.9) To train both institutional and department personnel on the proper function and use of all issued products, as necessary.

THE REORGANIZED PROGRAM

The entire reorganization effort from evaluation to planning to initial implementation, lasted 15 months (i.e., July 1983 to October 1984), when the new facility opened. During the first six months, needs were assessed and preliminary plans were formulated. During the next six months, those plans were refined and presented for formal approval. Hardware vendors were also contacted, selected, and employed. The hiring process also began. During the last three months, the members of the reorganized program were hired, oriented, and trained. Informal support was

pursued and institution-wide practices were phased in. On the actual date of the move to the new facility, the new security program was placed into full effect. It can be summarized as follows:

Overview

The security department was renamed the Department of Protective Services to reflect a new and enhanced role (which included firefighting, safety and disaster preparedness in addition to routine security and law enforcement functions). Arrest authority was granted and members were "sworn in" at a formal graduation ceremony following the training. This arrest authority made the program unique in the health care field. It became the first hospital security department in Michigan to be the equivalent of a public police department and only the fourth security program of any type to be so designated.

Firearms were issued under strict control, after successful completion of training and range qualifications. Considerable public exposure was provided in the health center's weekly and bi-weekly publications and "get acquainted" meetings were held with the hospital staff. All contract security guard agency services were terminated and the program became entirely proprietary or in-house.

People

The existing security personnel were given the first opportunity to compete for the newly created positions. Only 3 out of the original 36 qualified for the "sworn"

positions under the increased employment standards. (One of those eventually "washed out.") Several were actually discharged for misconduct during the 15 months before the reorganization took effect. The lower level Officer (i.e., Officer I) classification was totally eliminated and so its members were laid off. Fortunately, most of them were subsequently reassigned to other jobs in the health center. The remaining higher level Officers (i.e., Officer II) and Supervisors either took other jobs in the health center or else automatically became nonsworn Officers in the new program. The Dispatchers were selected from employees in other departments. The vast majority of the sworn Specialists, as well as all Supervisors and the Manager, were selected from outside the institution. (Many had actually worked for the author before at other jobs.)

All of the external candidates had "clean" police, employment, and driving records. Most had previous experience in security and/or law enforcement. All had been assessed as psychologically stable and drug-free. The Manager had a Master's Degree and had been a police lieutenant and an Under-sheriff. All of the Supervisors had Bachelor's Degrees and previous experience in law enforcement or hospital security. The remainder either had at least Bachelor's Degrees or some college, with experience in the field. In fact, nearly one-half of the external hirees had served as police officers at one time or another.

The racial composition of the reorganized department was roughly comparable to that of the previous one (i.e., 43 vs 45 percent black). However, a full one-third was now female and the average age was 16 years younger (i.e., 30). No one had physical nor psychological problems or limitations which interfered with job performance. All of the new members of the department were highly motivated and totally enthusiastic about the reorganization. Total department strength was reduced to 40 members, 16 previous health center employees and 24 external hirees. They were the most comprehensively trained and best paid hospital security personnel in the history of the state. All-in-all, they formed a nucleus which was unsurpassed in the field.

Property

Along with new people, new equipment and hardware were purchased and installed. Personal gear included a complete radio system which allowed everyone to carry a radio at all times. New firearms were provided, along with specially designed short-range ammunition, which would not "over-penetrate" walls or bodies (a major concern inside a hospital). Two fully equipped vehicles were purchased for patrolling the campus. One of them had four-wheel drive for use in snowy winter conditions. Uniforms were of two designs. Indoors, three-piece "business suit" type uniforms were employed to provide a "soft" approach. Outdoor posts and patrols required the more traditional "police" type uniform for visibility. Badges, nightsticks, and handcuffs

were also provided to sworn personnel. Finally, a reference library of legal materials, training aids, and procedural documents was developed (including a V.C.R. and tapes).

Major physical security hardware was state-of-the-art. In fact, it was as sophisticated as found in any other hospital in the state. High-pressure sodium vapor outdoor lighting was provided. It was computer designed to provide even, high-intensity fields of light. A decorative wrought-iron fence was installed around the edge of the property and "clear zones" were provided on both sides of the fence. Traffic flow patterns were restricted to two entrances with cul-de-sac drives. Bushes, trees, and other potential hiding places were kept away from walkways and building entrances.

A high-security lock and key system was installed. It was "mastered" by department, so that a lost or stolen master key would not jeopardize any area other than the department it came from. All keys were coded and recorded for easy identification.

Forty C.C.T.V. cameras were located throughout the health center. Outdoor cameras had "low-light" capability and were located so as to provide overlapping coverage. They had all-weather capability and were mounted on "bubbles," which reduced their visibility to the public. Indoor cameras were similarly mounted at key locations within the health center itself. A complete bank of monitors for the cameras was installed at a central dispatch

station. This included a base radio station, V.C.R., fire computer, and access control computer.

All parking lots were gate controlled. Visitors were directed to a single lot where they paid for parking. Employees and medical staff were assigned to separate lots based on their shift and location within the health center. These lots were accessed via I.D. cards, which also gained entrance to appropriate building entrances. These entrances also had card readers, which allowed only authorized personnel to enter at specified times.

With the exception of the visitors' and emergency room entrances, all other building doors were locked. In fact, all fire exists were locked from the inside (the first time the State Fire Marshall had permitted this) by magnetic locks which were tied to the fire alarm and computer system.

All building doors were alarmed and tied into the access control computer. In addition over 100 "hold-up" alarms were installed throughout the facility, at every nursing station, and high-risk areas (e.g., pharmacy, psych unit, etc.). Bulletproof glass was also installed at such locations.

Everything was computer controlled and monitored 24 hours a day. Aesthetics were a major consideration in order to avoid the image of an "armed camp." (A better listing of all major hardware components are contained in Appendix M.)

Practices

All of the institution-wide proposals listed earlier were eventually approved and implemented. A considerable amount of re-education and collaborative effort was necessary, but ultimately the majority of the health center employees and medical staff positively participated in the new security program.

The most effective technique for ensuring cooperation (and avoiding confrontations between security personnel and others) involved behavior modification. Working conditions were altered such that people had to cooperate. For example, in order to ensure compliance in the wearing of I.D. badges, they were developed to also have a card access function. In order to gain entry to a parking lot and employee entrance, the employees had to bring their I.D. badges to work, making it both convenient and necessary to wear them. Assignments to parking lots and employee entrances were computer programmed according to shift and work area in the health center. This allowed night shift employees to park in controlled areas close to the employee entrances and segregated employees from visitors, creating a much more manageable situation for monitoring and protecting the campus.

Key distribution and control also contributed to general security conditions. Keys were issued on a need-to-possess basis. Only department heads were given master keys. Everyone had to sign for their keys and return them

upon termination of employment or else forfeit their final paycheck. Lost keys were charged for and the department had to pay the cost of rekeying the door(s) involved.

Visitor control procedures were tightened and coordinated by security personnel. Metal detectors and full searches were used on all mental health patients (i.e., psychiatric and substance abuse) upon admission and on disruptive emergency room patients and visitors. Persons refusing to comply were required to leave the premises or else be arrested.

An employee property checkout procedure was implemented to ensure that health center property was recovered upon termination of employment (e.g., keys, I.D. badges, beepers, tools, etc.). A property removal authorization system was also put into place to make sure people weren't walking out of the health center with unauthorized items.

Procedures for recognizing and identifying criminal suspects were disseminated, as were the proper steps for requesting assistance from the security department. General security and safety tips were included in every health center newsletter. Finally, disciplinary rules giving the security department enforcement authority, were placed into effect.

SUMMARY

The process of evaluating the existing security program, designing a new one, and subsequently implementing it was a formidable task. This was especially true because

the existing security department had to be managed during the entire reorganization effort (no small task due to its poor condition) and considerable attention had to be also devoted to providing general security for the actual move to the new location. Nevertheless, the new program, with only a couple of exceptions, was put into place when the move occurred. It was curiously unique, somewhat controversial and completely untested. However, it represented a potentially large and radical improvement over other conventional hospital security programs.

Following the theoretical framework described in Chapter 3, this program was developed and implemented in a "high-risk" environment in a period of 15 months. Although some degree of "debugging" and minor revisions was necessary over the next few months, the revised program was basically complete in October 1984, the time of the move to the replacement facility and new location. In the next chapter, an analysis of the impact and results of that program over a two-year period will be provided.

CHAPTER 6

ANALYSIS

INTRODUCTION

In this chapter, the reorganized security program (as developed and implemented within the context of the theoretical framework described in Chapter 3) is evaluated. The general hypotheses (i.e., goals) are restated and their operational counterparts (i.e., objectives) are analyzed. Brief summaries are provided for each of the hypotheses. The overall results for 83 - 84 versus 84 - 85, and 84 - 85 versus 85 - 86 are also discussed. Finally, a general summary is presented, in which salient findings over the entire three-year period of the study are reviewed.

1983 - 84 VERSUS 1984 - 85

Hypothesis 1

Prevention of security . . . related incidents which may result in personal harm, property loss, legal liability, or disruption of routine health care operations.

1.1: To reduce the number of crimes against persons below 1983 - 84 levels.

The F.B.I.'s categories of major (i.e., Part I) crimes against persons may be described as homicide, felonious assault, criminal sexual conduct, and robbery. There are varying degrees in each category, but they are all combined

here. In addition to these categories, simple assault-and-battery has been added for further analysis. The figures presented in Table 6.1 reflect all such reported crimes for the year before the reorganization as well as the first year thereafter.

TABLE 6.1
MAJOR CRIMES AGAINST PERSONS

Category	Number of Crimes 83-84	84-85
Homicide	0	0
Felonious Assault	2	1
Criminal Sexual Conduct	1	0
Robbery	3	1
Assault and Battery	5	4
	11	6

While none of the numbers were large and the decreases were not dramatic, there was a general trend downward in all categories. Furthermore, the assault-and-battery numbers for 84 - 85 represented three assaults on nurses by aggressive patients, a statistic which had not been reported to security in the previous year. No serious injuries were reported.

As a result of these comparisons, this objective was met.

1.2: To reduce the number of property crimes below 1983 - 84 levels.

The F.B.I.'s categories of major crimes against property include larceny over $100, breaking-and-entering, auto theft and arson. In addition, the category of

malicious destruction of property has been added for further analysis. The figures presented in Table 6.2 indicate the reported numbers of these crimes over the two-year period.

TABLE 6.2
MAJOR CRIMES AGAINST PROPERTY

Category	Number of Crimes 83-84	84-85
Larceny over $100	42	34
Breaking & Entering	5	0
Auto Theft	8	6
Arson	1	0
Destruction of Property	10	11
	66	51

Breakings-and-enterings were completely eliminated. Major larcenies were reduced noticeably, if not significantly. Interestingly enough one-half of these larcenies for 84 - 85 occurred during the first four months (i.e., October - January), a period when part of the access control and CCTV systems were not fully installed yet. More specifically the majority of these losses occurred from parked vehicles, which were not yet under camera surveillance nor in appropriate parking lots with gate access. Likewise, five of the six vehicles stolen were parked in similar places. After full control was established, this problem stopped. The one remaining auto theft was foiled before the perpetrator could get away. Only malicious destruction of property (i.e., mostly broken windows) did not show a decrease and the author was informed

that at the older facilities this was seldom reported at all.

One statistic which is not included in the table involves larcenies under $100. Only 31 occurrences of "minor" theft were reported in the year prior to the reorganization (an incredibly small amount for any hospital). This compared to 174 in the first year afterwards, when complete reporting and record-keeping were initiated. Historically, such crimes were almost never reported to the security department and so they have not been factored into this analysis.

Even though a couple of "qualifiers" were necessary in this analysis, major property crimes were indeed reduced. Therefore, this objective was met.

1.3: To reduce the amount of monetary losses associated with all crimes before 1983 - 84 levels.

The dollar amounts of losses from theft, robbery, and other crimes have been combined for each year and are compared in Table 6.3.

TABLE 6.3
MONETARY LOSSES FROM CRIME

	83-84	84-85	%(+/-)
Amount Stolen	$120,000	$ 89,413	-25.5

For 83 - 84 the figure only reflects the value of losses from robbery, auto theft, and larceny over $100. It is a conservative estimate, based on incomplete reporting.

However, the 84 - 85 figure is more accurate and even includes all the larcenies under $100. In spite of this, there was a dramatic decrease by 25 percent in reported loss.

This objective was met.

1.4: To establish a per capita crime rate which is lower than that for the surrounding community.

According to 1980 census tract data, the population of the adjacent neighborhood to the new hospital was approximately 8,000. The average daily population at the hospital was approximately 1,600. Detroit Police Department crime statistics for the same census tract area were obtained and a ratio of crimes per 1,000 people was then calculated. The same was done for the crimes at the hospital. The comparisons are shown in Table 6.4. The categories listed in the table reflect the only types of crime statistics available from the police.

TABLE 6.4
RATIO OF CRIMES PER 1,000 PEOPLE

Category	Number of Crimes		Ratio Per 1000 People	
	Hospital	Neighborhood	Hospital	Neighborhood
Homicide	0	4	0.0	.5
Criminal Sexual Conduct	0	6	0.0	.75
Robbery	1	100	.63	12.5
All Assaults	5	40	3.13	5.0
Breaking and Entering	0	125	0.0	15.63
Larcenies Over $100	34	152	21.25	19.0
Auto Theft	6	106	3.75	13.25
	46	533	28.75	66.63

With the exception of larcenies, the ratio of crimes per 1,000 people was considerably lower in 84 - 85 at the

hospital than for the surrounding community in all categories. The small discrepancy in larcenies may be partially attributed to the fact that larcenies often go unreported to the police in the City of Detroit. However, even if this were not the case the overall ratio of crimes per 1,000 people at the hospital was less than one-half that of the neighborhood.

This objective was met.

Summary. All four objectives were met, resulting in the goal being achieved. The reorganized security program was generally able to prevent the occurrence of crime in a "higher risk" environment than the older security program had operated in. Therefore, Hypothesis 1 is accepted.

Hypothesis 2

Minimization of the degree of harm, loss, liability or disruption associated with those incidents which cannot be prevented.

2.1: To effectively control all occurrences of crimes still in progress once a response is made without additional injury to innocent persons or further avoidable monetary loss/property damage.

This is admittedly an ambitious objective that must be evaluated with subjective judgment. It basically means that whenever security personnel arrive at the scene of a crime in progress they handle the situation effectively without any further injuries to anyone (other than possibly themselves or the perpetrators) and without letting the perpetrators get away with stolen property. The most common

examples of such crimes are larcenies, people carrying and displaying weapons, and "disorderly" or combative persons.

Literally dozens of such incidents occurred. In each case the responding security personnel were successful. Therefore, this objective was met.

2.2: To recover a larger percentage of stolen property (i.e., amounts) than during 1983 - 84.

This refers to either catching a thief in the act or else recovering stolen property through follow-up investigation and/or aggressive patrol. The comparisons are shown in Table 6.5. They include all thefts due to robbery, auto theft, breaking and entering, and overall larceny.

TABLE 6.5
RECOVERED STOLEN PROPERTY (AMOUNTS)

Year	Number of Thefts	Number of Recoveries	%
83-84	89	2	2.2
84-85	215	16	7.4

Even though the actual number of larcenies under $100 was undoubtedly under-reported for 83 - 84, the more accurate figures for 84 - 85 still reveal a significant increase in the number and percentage of recoveries.

This objective was met.

2.3: To recover a larger percentage of stolen property (i.e., monetary value) than during 1983 - 84.

A comparison of the relative dollar value of the stolen property recovered in 83 - 84 versus 84 - 85 is shown in Table 6.6.

TABLE 6.6
RECOVERED STOLEN PROPERTY (VALUES)

Year	Value of Thefts	Value of Recoveries	%
83-84	$120,000	$ 150	.13
84-85	$ 89,413	$11,902	13.31

In 83 - 84 only two stolen items valued at approximately $150.00 were recovered. In 84 - 85 there were 16 recoveries made, valued at $11,902.00. This represented a dramatic increase over 83 - 84 (i.e., over 13 percent versus less than 1 percent).

This objective was met.

2.4: To apprehend a larger percentage of offenders committing crimes than during 1983 - 84.

A comparison for this objective is difficult to make because the security personnel in 83 - 84 did not have the legal authority to make arrests. Practically speaking, however, this did not deter them from holding someone if they could catch them until the Detroit Police arrived.

In Table 6.7 a comparison is made of the apprehensions made by the security department in 83 - 84 versus the number of formal arrests made by the reorganized department in 84-85. They refer to the crimes listed in Tables 6.1 and 6.2.

TABLE 6.7
APPREHENSIONS MADE

Year	Number of Crimes	Number of Apprehensions	%
83-84	77	2	2.60
84-85	57	6	10.53

The comparison clearly shows that the security department in 84 - 85 was more successful in apprehending criminals than in 83 - 84 (i.e., over 10 percent versus 2 percent). However, this only pertains to the categories of serious crimes for which there was comparable data in both years (i.e., Tables 6.1 and 6.2). It actually understates the overall success of the department in 84 - 85 because other categories of crimes for which arrests were made (including all misdemeanors) are not included. Neither are certain apprehensions which did not result in formal arrests. Examples of these include patients caught stealing (the hospital wouldn't ordinarily prosecute), people caught with an illegal knife or other weapon (unless it was a firearm), and people caught with illegal drugs (unless there was intent to sell). These figures will be presented when comparisons between 84 - 85 and 85 - 86 are made.

This objective was met.

Summary. All four objectives were met, resulting in the goal being achieved. The reorganized security program was able to reduce (i.e., minimize) the degree of loss and harm associated with crimes and security-related incidents which

were not prevented from initially occurring. Therefore, Hypothesis 2 is accepted.

Hypothesis 3

Correction and/or elimination of the underlying problems which either cause or allow incidents to initially occur.

3.1: To investigatively solve a larger percentage of initially unsolved crimes than during 1983 - 84.

This is another objective for which comparisons are difficult for all crimes. The jurisdiction of the security department, both before and after the reorganization, was limited to hospital property itself. If an unknown perpetrator escaped to the surrounding community, the matter of investigative follow-up was by necessity turned over to the Detroit Police Department. Therefore, follow-up investigations were primarily (but not exclusively) limited to certain employee or patient-related crimes, such as larceny.

No crimes were solved by the security department in 83 - 84 in which the perpetrator was neither initially caught nor identified at the scene. However, eight cases of larceny were solved by security personnel in 84 - 85, resulting in discharge and/or prosecution.

This objective was met.

3.2: To investigatively identify all unsafe conditions and practices which contributed to the occurrence of crimes and to present specific, corrective recommendations for preventing their recurrences.

Whenever a crime or security-related incident was reported in 83 - 84, it was simply filed and forgotten. Little or no effort was made to diagnose the underlying problem, if it was not blatantly obvious. However, in 84-85 it became standard procedure for the security Specialist taking a report to also conduct a preliminary investigation into the potential cause(s) which might have contributed to the incident. Each and every report was then reviewed by the Manager and/or the author to further analyze the source of the problem in terms of time frames, system components and levels of analysis (according to the Systems View guidelines described in Chapter 3). Recommendations for corrective countermeasures were then developed and proposed as appropriate.

This objective was met.

3.3: To ensure that all corrective recommendations for crimes . . . are fully implemented, once the appropriate approvals are received.

Most of the recommendations made were approved by the appropriate authorities for implementing. Periodic follow-up and monitoring were made to ensure this occurred properly. In almost every case, where a specific recommendation was made and implemented, there were no recurrences of incidents.

This objective was met.

Summary. All three objectives were met, resulting in the goal being achieved. To a large degree, the investigative follow-ups and subsequent implementation of recommendations

were a continuation of the Evaluation-Planning-Execution processes associated with the ACTION MODEL. They constituted a "debugging" of the original reorganized program (which was quite successful as will be shown in the 84 - 85 versus 85 - 86 comparisons). Therefore, Hypothesis 3 is accepted.

Hypothesis 4

Provision of those miscellaneous services required for the general welfare and efficient operations.

4.1: To provide a broader range of miscellaneous "helping" services and general assistance to the institution than during 1983 - 84.

This objective was met. After the reorganization, the scope of services of the department was greatly expanded. (This is further elaborated in Hypothesis 14.1)

4.2: To provide in-service training to health center staff in the following areas:

Physical Management of "Disturbed" Persons
Fire Protection and Response
Tornado Protection and Response

This objective was met.

4.3: To provide to health center staff the following loss prevention related services for personal use:

Vehicle Etching
Security, Safety and Fire Protection Pamphlets

This objective was met.

4.4: To fully implement, administer, and maintain the following loss prevention programs:

Access and Parking Control
Key Control
I.D. Badge
Vehicle Registration
Property Removal Pass
Operation I.D. of Health Center Property
Lost and Found

This objective was met.

4.5: To provide active participation in the following community-wide crime prevention programs and activities associated with the Warren/Connor Coalition:

Youth-on-Edge
Anticrime Task Force
Cops-and-Neighbors
Neighborhood Security Patrol

This objective was met (and the department received a letter of commendation for its participation).

4.6: To develop and implement a revised "New Employee Orientation" program on security.

This objective was met.

4.7: To develop and implement a patient security program as part of the institution's patient eduction service.

This objective was not met.

Summary. Six of the seven objectives were met. The seventh involved the development of a television program on security for patients to watch. It was never produced for economic reasons. However, the overall goal for the department to provide needed miscellaneous services was achieved. Therefore, Hypothesis 4 is accepted.

Hypothesis 5

The effective acquisition, development, and maintenance of all departmental resources.

5.1: To actively maintain at all times a manpower pool of qualified job applicants in each job classification.

This objective was met.

5.2: To maintain "standing" manpower levels at all times which satisfy the institution's staffing needs.

This objective was met.

5.3: To utilize a fair and effective selection process which includes job specific criteria, fingerprinting and police background checks, job reference checks, psychological assessment, structured interviews, and employment testing.

This objective was met (as judged by the hospital's labor attorneys).

5.4: To develop and utilize fair and effective promotional process which includes analysis of work records, structured interviews and assessment centers.

This objective was met (as judged by the hospital's labor attorneys).

5.5: To provide active recruitment, selection and promotion of qualified applicants in accordance with all applicable civil rights legislation.

This objective was met (as judged by the Michigan Department of Civil Rights, independent arbitrators, and the hospital's grievance panel after several challenges by unqualified candidates).

5.6: To maintain a racial and sexual composition of department members which reflects that of the community and the institution.

A standard was set by the author's supervisor (the Vice President of Human Resources who was a black man). It required that department personnel must be at least 40 percent black and 20 percent female. The actual composition ended up being 43 percent black (and Hispanic) and 32 percent female. White males were actually in the minority.

This objective was met.

5.7: To develop and utilize a comprehensive department policy and procedure manual, which describes all job duties and expectations for all job classifications.

This objective was met.

5.8: To conduct and continually revise an effective basic training program for all employees which consists of no less than 80 hours of classroom and O.J.T. instruction and also includes both written and practical application examinations.

This objective was met.

5.9: To conduct and continually revise an effective advanced trained program for "sworn" employees which consists of no less than 130 hours of classroom and field instruction and also includes both written and practical application examination.

This objective was met.

5.10: To provide additional job-specific training to all employees on an "as needed" basis.

This objective was met.

5.11: To provide supervisory and management personnel with additional "professional development" training.

This objective was met.

5.12: To maintain the institution's computerized security system in good working order at all times.

This objective was met.

5.13: To maintain all department hardware and equipment in good working order at all times.

This objective was met.

5.14: To maintain accurate up-to-date department records at all times.

This objective was met.

Summary. All 14 objectives were met resulting in the goal being achieved. Therefore, Hypothesis 5 is accepted.

Hypothesis 6

The effective utilization and management of all existing department resources.

6.1: To maintain adequate shift coverage and duty assignments at all times, according to the institution's needs.

This objective was met.

6.2: To identify changing institutional needs and provide both adequate resources and effective procedural responses to them.

This objective was met.

6.3: To establish and maintain a "participative management" approach to routine decisionmaking involving employee input and advice.

This objective was met.

6.4: To adhere to all applicable laws, policies, procedures, rules and regulations pertaining to the management and utilization of department resources at all time.

This objective was met.

6.5: To assign, supervise, discipline, and reward personnel in a fair and equitable manner at all times.

This objective was met.

6.6: To provide performance planning assistance to all personnel and to administer performance appraisals on an annual basis.

This objective was met.

6.7: To satisfactorily pass all external and internal audits pertaining to department operations, effectiveness, and management.

The department was inspected by an outside consulting firm as part of a review of the entire hospital. It made no recommendations for improvement, staff reductions nor budget cuts. Instead, it commended the entire program. Furthermore, due to the fact that the department was licensed to have arrest authority, the Michigan State Police inspected it twice (i.e., biannually) to ascertain that it operated in an effective and entirely legal manner. In both cases, the department was found to have no violations of State Police standards and to be operating professionally. Finally, the whole program was internally reviewed by the administrative staff (due to the controversial nature of its original inception). No major criticisms were made at all, but rather compliments were given.

This objective was met.

6.8: To thoroughly investigate all complaints and concerns made about the department and take the appropriate remedial actions in a timely fashion.

This objective was met.

Summary. All eight objectives were met, resulting in the goal being achieved. Therefore, Hypothesis 6 is accepted.

Hypothesis 7

Adherence to fiscal constraints on departmental resources in a cost-efficient manner.

7.1: To operate within approved budgetary allocations for the year.

This objective was met.

7.2: To formulate and justify an annual budget request which is accurate and satisfies the department's actual fiscal needs without unnecessary expense to the institution.

This objective was met.

7.3: To demonstrate cost-justification for all expenses incurred.

This objective was met.

7.4: To generate at least $35,000.00 in parking revenue for the institution during the year.

This objective was met.

Summary. All four objectives were met, resulting in the goal being achieved. Therefore, Hypothesis 7 is accepted.

Hypothesis 8

A healthy organizational climate within the department which fosters positive working relationships and teamwork.

8.1: To improve department self-perceptions in terms of morale and performance over the previous recorded levels.

Several measures were employed. Surveys were conducted in July 1983 and June 1985. In 1983, 33 of the 36 members of the department were present when the survey was administered. Unfortunately, only 14 chose to participate and some of them didn't answer all of the questions. In 1985, there were 34 out of 40 members present for the survey and all of them participated.

The survey inquired into several areas. First, 12 different categories were assessed on a Likert scale from "Poor" to "Excellent" (i.e., 1 to 5 numerically). In Table 6.8 the results are shown of T-Tests of the differences in means on these criteria over the two surveys.

TABLE 6.8
OVERALL SELF-PERCEPTIONS

	83-84			84-85			
	n	$\bar{x}$	s	n	$\bar{x}$	s	T-Value
Public Relations	10	2.80	1.03	33	3.73	.84	-2.90*
Crime Prevention	10	2.40	.97	33	3.79	.82	-4.50*
Investigative Skills	10	2.30	1.06	34	3.76	.89	-4.38*
Crisis Intervention	9	2.56	.89	33	4.36	.60	-7.20*
Communication Skills	9	2.44	1.01	34	4.00	.78	-5.00*
Job Knowledge	9	2.44	1.01	34	4.00	.70	-5.40*
Dedication/Interest	10	2.30	1.25	33	3.73	.84	-4.18*
Professional Demeanor	9	2.33	.87	33	3.97	.73	-5.74*
Response Time	9	3.56	1.13	33	4.64	.74	-3.44*
Miscellaneous Services	10	2.70	.95	33	4.18	.81	-4.88*
Overall Image	10	2.70	.82	33	4.24	.61	-6.42*
Overall Performance	10	2.80	.79	31	4.19	.65	-5.57*

*Significant at $\alpha = .05$

$\bar{x}$		INTERPRETATION
0.0 to 1.49	=	Poor
1.5 to 2.49	=	Needs Improvement
2.5 to 3.49	=	Adequate
3.5 to 4.49	=	Good
4.5 to 5.0	=	Excellent

In spite of the small number of respondents in 1983, the results clearly indicate significant improvements in the department's self-perceptions in every category. Interpreted verbally, the respondents in 1983 evaluated the department as "Needs Improvement" or "Adequate" in every area. In 1985, the department rated itself as "Good" in every area except for Response Time which was considered "Excellent."

The issue of overall departmental morale was also assessed on a 1 - 10 scale. It was found to be significantly higher in 1985, as shown in Table 6.9.

TABLE 6.9
DEPARTMENT MORALE

83-84			84-85			T-Value
n	$\bar{x}$	s	n	$\bar{x}$	s	
14	5.29	1.44	30	7.33	1.40	-4.49*

*Significant at $\alpha = .05$

Less sophisticated comparisons were also made. Respondents were asked to indicate their overall satisfaction with the quality of services provided by the department. This was done with a multiple-choice question, as shown in Table 6.10.

Whereas in 1983 a full one-half of the respondents expressed some level of dissatisfaction with the quality of services provided by the department, only one respondent indicated the same in 1985. Interestingly enough, this

individual identified himself and the reason for his dissatisfaction. He was one of the Security Officers before the reorganization and was upset because he hadn't been selected to be a sworn Specialist in the new program. However, the remaining 33 respondents indicated personal satisfaction. Over one-half were "Almost Always Satisfied."

TABLE 6.10
SATISFACTION WITH QUALITY OF SERVICES

	83-84		84-85	
	n	%	n	%
Almost Always Satisfied	3	25	19	56
Generally Satisfied	3	25	14	41
Generally Dissatisfied	6	50	0	0
Almost Always Dissatisfied	0	0	1	3

Three additional multiple-choice questions were asked in 1985. The first one asked how the reorganized department compared to one year earlier (i.e., before the reorganization). The results are shown in Table 6.11.

TABLE 6.11
OVERALL COMPARISON TO PREVIOUS YEAR

	n	%
Much Improved	15	45
Slightly Improved	6	18
About the Same	0	0
Slightly Worse	0	0
Much Worse	0	0
Don't Know	12	37

Over one-third of the respondents had no opinion, because they were hired as part of the reorganization itself. However, the remainder were unanimous in stating that the new security department was better than the old one.

Another question dealt with rating the reorganized department relative to expectations for the new location. The results are shown in Table 6.12.

TABLE 6.12
EXPECTATIONS OF THE DEPARTMENT

	n	%
Greatly Exceeds Expectations	4	13
Somewhat Exceeds Expectations	17	53
Meets Expectations	10	31
Somewhat Fails to Meet Expectations	1	3
Greatly Fails to Meet Expectations	0	0

Ninety-seven percent of the respondents stated that the reorganization program either met or exceeded their expectations. The only dissenter was the person who had not been promoted to Specialist level.

The last question asked department personnel if they felt safe at work themselves. Thirty-three responded and all of them indicated that they did indeed feel safe, in spite of the environment and problems they had to encounter daily.

The survey results unequivocally reveal that the new security department held itself in higher regard in all

areas than before the reorganization. Therefore this objective was met.

8.2: To reach consensus on department related problems and their solutions via department-wide participation in the hospital's organizational climate survey.

This objective was met.

8.3: To positively reward overall performance by matching performance ratings with merit salary increases in a fair and equitable manner.

This objective was met.

8.4: To reward outstanding achievements through the development and successful implementation of a department "awards" program.

The intent of this objective was to provide formal recognition (e.g., ribbons and medals) much like the military and public police. While letters of commendation were provided for valor and merit, a formal awards program was not developed.

This objective was not met.

Summary. Three of the four objectives were met, resulting in the goal being achieved. Therefore, Hypothesis 8 is accepted.

Hypothesis 9

A positive image of the department within the health center and community which promotes confidence, trust, cooperation, and favorable public relations.

9.1: To improve the institution's perceptions of the department in terms of its overall performance, image, and professionalism over previous recorded levels.

The survey data obtained from the security department in 1983 and 1985 were also solicited form the hospital's total management team at the same times. This group consisted of administrators, some physicians, department heads, managers, and supervisors. One-hundred and five responded in 1983 and 73 in 1985.

In Table 6.13 the overall management view is shown of the security department, both before and after the reorganization, in terms of the same categories that the department evaluated itself.

TABLE 6.13
OVERALL EMPLOYEE PERCEPTIONS

	83-84			84-85			
	n	x	s	n	x	s	T-Value
Public Relations	101	2.39	.77	69	3.72	.77	-11.12*
Crime Prevention	90	2.13	.69	69	3.68	.74	-13.60*
Investigative Skills	85	2.08	.71	60	3.63	.61	-13.71*
Crisis Intervention	86	2.24	.83	61	3.82	.79	-11.63*
Communication Skills	99	2.24	.77	69	3.80	.70	-13.36*
Job Knowledge	88	2.33	.74	67	4.04	.71	-14.60*
Dedication/Interest	92	2.39	.86	68	3.99	.64	-12.86*
Professional Demeanor	92	2.03	.76	71	4.10	.76	-17.19*
Response Time	88	2.69	.91	66	3.85	.90	- 7.82*
Miscellaneous Services	87	2.71	.81	64	3.80	.74	- 8.46*
Overall Image	96	2.23	.80	72	3.92	.69	-14.35*
Overall Performance	96	2.28	.71	71	3.93	.54	-16.40*

*Significant at $\alpha = .05$

$\bar{x}$		INTERPRETATION
0.0 to 1.49	=	Poor
1.5 to 2.49	=	Needs Improvement
2.5 to 3.49	=	Adequate
3.5 to 4.49	=	Good
4.5 to 5.0	=	Excellent

The findings clearly reveal that there were significant improvements in employee attitudes toward the reorganized

security department in all categories. In 1983, the department was rated as "Adequate" in only two areas, Response Time and Miscellaneous Services. The remainder were assessed as "Needs Improvement." However, in 1985 these ratings increased to "Good" in every area.

The employee satisfaction levels with the quality of services provided by the security department are shown in Table 6.14.

TABLE 6.14
SATISFACTION WITH QUALITY OF SERVICES

	83-84		84-85	
	n	%	n	%
Almost Always Satisfied	3	3	34	47
Generally Satisfied	43	43	39	53
Generally Dissatisfied	49	49	0	0
Almost Always Dissatisfied	6	6	0	0

In 1983, over one-half of the respondents were basically dissatisfied with the quality of services rendered by the department. However, in 1985 no overall dissatisfaction was registered at all. In fact, nearly one-half of the respondents were "Almost Always Satisfied," as opposed to only three in 1983.

Three posttest-only questions were also asked of this group in 1985. The first one dealt with how well the new department compared overall to a year earlier (i.e., before the reorganization). The results are shown in Table 6.15.

Several of the respondents could not compare the department to the previous year because they had not worked at the hospital before the reorganization. However, the remainder was unanimous in appraising the department as being better than before. In fact over two-thirds considered it "Much Improved."

TABLE 6.15
OVERALL COMPARISON TO PREVIOUS YEAR

	n	%
Much Improved	46	69
Slightly Improved	12	18
About the Same	0	0
Slightly Worse	0	0
Much Worse	0	0
Don't Know	9	13

When asked how well the new department met with their original expectations for it, the respondents were also generally impressed, as revealed in Table 6.16.

TABLE 6.16
EXPECTATIONS OF THE DEPARTMENT

	n	%
Greatly Exceeds Expectations	17	25
Somewhat Exceeds Expectations	20	29
Meets Expectations	31	45
Somewhat Fails to Meet Expectations	1	1
Greatly Fails to Meet Expectations	0	0

Out of 69 respondents, only one indicated that the new department failed to meet his/her expectations. Over one-

half felt it exceeded their original expectations and the rest stated it met them.

The last question asked how the new department compared to other hospital security departments that the respondents might be familiar with (from working in other health care institutions). The results are shown in Table 6.17.

TABLE 6.17
COMPARISON TO OTHER HOSPITAL SECURITY DEPARTMENTS

	n	%
Much Better	28	41
Slightly Better	14	21
About the Same	9	13
Slightly Worse	1	1
Much Worse	0	0
Don't Know	16	24

One-fourth of the respondents could not compare the department to those of other institutions. However, 62 percent felt it was better than other programs they were familiar with. Thirteen percent rated it the same, and again only one person expressed a negative view.

Admittedly, but by necessity, only management personnel were included in the surveys. However, the findings indicate a definite improvement in their opinions of the security department after the reorganization. Therefore, this objective was met.

9.2: To reduce the institution's overall level of fear related to crime at the institution's new location.

Direct comparisons before and immediately after the reorganization of the security program (and move to the new location) were not possible. Hospital-wide surveys specifically addressing security were not permitted. However, inferences can be drawn from some of the data which were available.

In the July 1983 survey of the total management team, the respondents voiced their concerns over the impending move. Sixty-two percent indicated concern that crime would be worse at the new location than at the two existing ones. The remainder either thought crime levels would be the same or else had no opinion. Ninety-three percent felt that a better security program was vital to the survival of the institution once the move was made. These sentiments were echoed by the general employee population (even though no hard statistics were kept in this regard). In fact, security was widely considered the single biggest concern associated with the move.

In January 1985 (only four months after the reorganization and move), a hospital-wide survey was conducted by the Personnel Department to assess a variety of issues dealing with the move and the general organizational climate. One question on security was allowed. Of the 1,100 respondents, only 29 percent still had any level of concern for their personal safety with the new security department in place. Forty-nine percent no longer were concerned about security and the rest had no opinion.

In June 1985, the total management team was again surveyed. Out of 69 respondents, only two still felt unsafe at work. Ninety-seven percent indicated they felt safe.

Any conclusion derived from these findings must be interpreted inferentially and with caution. However, the available evidence would tend to indicate that the employee population was no longer afraid to work at the new location, in spite of previous fears before the move.

This objective was met.

9.3: To maintain positive working relationships at all times with other segments of the institution, patients, visitors, and physicians with whom contact is made.

This objective was met.

9.4: To maintain positive working relationships at all times with local criminal justice, fire, and community agencies/organizations with whom contact is made.

This objective was met.

Summary. All four objectives were met, resulting in the goal being achieved. Therefore, Hypothesis 9 is accepted.

Hypothesis 10

Effective communication links both within the department and the health center.

10.1: To disseminate all information necessary for effective operations on a daily basis at shift briefings.

This objective was met.

10.2: To provide complete, up-to-date and timely instructions on all new or revised policies, procedures, rules and regulations which pertain to department personnel.

This objective was met.

10.3: To conduct periodic department-wide meetings for the purpose of joint planning, problem-solving and information sharing.

This objective was met.

10.4: To conduct periodic "management team" meetings for the purpose of joint planning, problem-solving, information sharing and coordinating of routine operations.

This objective was met.

10.5: To provide timely status reports to the appropriate authorities on department operations, individual incidents, emerging problems, and alternative solutions.

This objective was met.

10.6: To provide active participation on all assigned committees/task forces and at all relevant meetings conducted by the health center.

This objective was met.

10.7: To disseminate security . . . information and instructions to all affected personnel in the institution whenever necessary.

This objective was met.

Summary. All seven objectives were met, resulting in the goal being achieved. Therefore, Hypothesis 10 is accepted.

1984 - 85 Results

There are 10 goals (i.e., general hypotheses) and 59 objectives for the 84 - 85 period. Many objectives are non-quantitative and only 10 involve direct pretest-posttest comparisons with the 83 - 84 period. However, the findings quite clearly indicate the overall success of the reorganized security program.

Crime actually decreased in an environment where it was expected to increase. Employee attitudes toward the security department improved dramatically. The department's own self-perceptions increased. Employees generally felt safe at work.

All 10 goals were achieved and 57 of the 59 objectives were met. Using the formula described in Chapter 4, the security program could have been given a possible total of 77 points for overall effectiveness. It actually received 74 points for an effectiveness rating of 96.1 percent.

Given the possibility that the findings for the 84 - 85 period were simply a "fluke" associated in some way with the move to the new location (e.g., a Hawthorne effect), an analysis of the reorganized security program for the 85 - 86 period was also made. The goals remained the same, but some of their corresponding objectives were even more ambitious. It was believed that the program had been sufficiently "debugged" by this point, so the findings from 85 - 86 would be indicative of the ultimate success or failure of the program.

1984 - 85 VERSUS 1985 - 86

Hypothesis 11

Prevention of security . . . related incidents which may result in personal harm, property loss, legal liability or disruption of routine health care operations.

11.1: To reduce the number of crimes against persons below 1984 - 85 levels.

In Table 6.18 a comparison is shown of the number of violent crimes committed at the new location in the 85 - 86 period (i.e., the second year) as opposed to the 84 - 85 period (i.e., the first year).

TABLE 6.18
MAJOR CRIMES AGAINST PERSONS

Category	Number of Crimes 84-85	85-86
Homicide	0	0
Felonious Assault	1	0
Criminal Sexual Conduct	0	0
Robbery	1	0
Assault and Battery	4	3
	6	3

All major violent crimes were eliminated. Only three misdemeanor assaults were recorded. These did not involve serious injuries.

This objective was met.

11.2: To reduce the number of property crimes below 1984 - 85 levels.

TABLE 6.19
MAJOR CRIMES AGAINST PROPERTY

Category	Number of Crimes 84-85	85-86
Larceny over $100	34	13
Larceny under $100	174	95
Breaking & Entering	0	0
Auto Theft	6	1
Arson	0	0
Destruction of Property	11	10
	225	119

A comparison of property crimes is made in Table 6.19. Due to better reporting and record-keeping after the reorganization of the security program, it is also possible to compare larcenies under $100 in the table.

"Major" larcenies were reduced by nearly two-thirds, "minor" larcenies by nearly one-half. Auto thefts were nearly eliminated altogether. Vandalism remained relatively constant. Overall property crimes were down by 47 percent.

Two interesting comments should be made. First, a large proportion of the larcenies under $100 involved stolen patient telephones (i.e., 77 in 84 - 85 and 51 in 85 - 86). At about the same time the hospital moved to its new location, the "breakup" of A.T. & T occurred. Among other things, this resulted in consumers having to purchase their own telephones. (Previously, the phones were the property of A.T. & T.) Patients began stealing their telephones for use at home, when they were discharged. Second, the only auto theft in 85 - 86 occurred on the same day, at the same time, in the same parking lot as the last auto theft in 84-85. It was theorized that the same person committed both thefts.

The objective was met.

11.3: To reduce the amount of monetary losses associated with all crimes below 1984 - 85 levels.

A comparison of the actual dollar value of losses associated with crime over the first and second years of the reorganized security program is shown in Table 6.20.

TABLE 6.20
MONETARY LOSSES FROM CRIME

	84-85	85-86	%(+/-)
Amount Stolen	$ 89,413	$ 17,129	-80.8

Losses were reduced by over 80 percent. Most of this could be attributed to a reduction in auto thefts, but all non-auto losses were down also.

This objective was met.

11.4: To maintain a per capita crime rate which is lower than that for the surrounding community.

The Detroit Police crime statistics for the immediate neighborhood in 85 - 86 are no longer available for publication, so ratio comparisons cannot be presented here. However, when they were made the results revealed a much lower per capita crime rate for the hospital than for the neighborhood in all categories. They were even lower than for the 84 - 85 period.

This objective was met.

Summary. All four objectives were met, resulting in the goal being achieved. Crimes and economic losses were further reduced from 84 - 85 levels. Therefore, Hypothesis 11 is accepted.

Hypothesis 12

Minimization of the degree of harm, loss, liability, or disruption association with those incidents which cannot be prevented.

12.1: To effectively control all occurrences of crimes still in progress once a response is made without additional injury to innocent persons or further avoidable monetary loss/property damage.

As in 84 - 85, departmental personnel were able to effectively intervene without losing control of any situation. Whenever a criminal perpetrator was personally confronted, he neither escaped, injured any innocent by-standers, nor further damaged property. In effect in every case where the department arrived at the scene of a crime in progress, that crime was successfully stopped with no additional loss or harm.

This objective was met.

12.2: To recover a larger percentage of stolen property (i.e., amounts) than during 1984 - 85.

Due to better reporting and record-keeping, the comparisons are more accurate than for 83 - 84 versus 84-85. These more reliable figures are shown in Table 6.21.

TABLE 6.21
RECOVERED STOLEN PROPERTY (AMOUNTS)

Year	Number of Thefts	Number of Recoveries	%
84-85	215	16	7.4
85-86	109	26	23.9

In spite of a smaller number of larcenies actually committed, more items were recovered before they could be removed from the hospital grounds. Approximately 24 percent of all thefts involved the thief being caught with the property, considerably more than in 84 - 85.

This objective was met.

12.3: To recover a larger percentage of stolen property (i.e., monetary value) than during 1984 -85.

In Table 6.22 a comparison is shown of the relative dollar value of the stolen property recovered in 85 - 86 versus 84 - 85.

TABLE 6.22
RECOVERED STOLEN PROPERTY (VALUES)

Year	Value of Thefts	Value of Recoveries	%
84-85	$ 89,413	$11,902	13.31
85-86	$ 17,129	$ 3,515	20.52

While the actual dollar amount of recoveries in 85 - 86 was less than in 84 - 85, the overall loss-to-recovery percentage was greater (i.e., over 20 percent versus over 13 percent). There was simply less stolen to recover.

An interesting comment should be made. It is a commonly accepted practice for police departments to include in their statistics recovered property which had not actually been stolen within their own jurisdictions. The most common example of this is the recovery of an auto which was stolen somewhere else. In 85 - 86 security department

personnel recovered two such vehicles and arrested the drivers. If the dollar values of those recoveries had also been factored into these "recovery" statistics then the department would have actually recovered more than had been stolen at the hospital (i.e., $17,715 recovered versus $17,129 stolen).

This objective was met.

12.4: To apprehend a larger percentage of offenders committing crimes than during 1984 - 85.

Due to the poor reporting and record-keeping before the reorganization, only those apprehensions for serious crimes were able to be compared in 83 - 84 versus 84 - 85. However, more complete numbers are available for 84 - 85 versus 85 - 86. Two types of comparisons are possible. The first deals with the number of formal arrests made relative to the number of crimes reported. The second relates to the number of illegal weapons and drugs confiscated by security personnel where no arrest was made.

The arrest rates for all reported crimes (with the exception of weapons and drugs) are shown in Table 6.23. It includes a variety of misdemeanor crimes not addressed in previous analyses (e.g., disorderly persons).

TABLE 6.23
ARREST RATES

Year	Number of Crimes	Number of Arrests	%
84-85	274	11	4.0
85-86	154	18	11.7

Even though fewer crimes were reported in 85 - 86 than in 84 - 85, departmental personnel were still able to arrest a greater number and percentage of perpetrators. (In neither period were any of these arrests subsequently determined to be improper or illegal.)

The number of confiscations of weapons and drugs from patients, visitors, and employees are shown in Table 6.24. Although possession of these contraband items was technically illegal, it was department policy not to arrest nor prosecute for mere possession. (Only if a person tried to use a weapon or sell drugs was an arrest made.)

TABLE 6.24
CONFISCATIONS OF CONTRABAND

	84-85	85-86	%(+/-)
Weapons	40	46	+15.0
Drugs	17	28	+64.7

More illegal drugs and weapons were confiscated in 85-86 than in 84 - 85. Most were taken from patients. However, some were taken from people who were either disorderly or else suspects in other crimes.

This objective was met.

Summary. All four objectives were met, resulting in the goal being achieved. The amount of loss associated with crimes which couldn't be prevented was further reduced from 84 - 85 levels. More property was recovered and more

criminals apprehended. Security personnel successfully handled every security-related situation they responded to. Therefore, Hypothesis 12 is accepted.

Hypothesis 13

Correction and/or elimination of the underlying problems which either cause or allow incidents to initially occur.

13.1: To investigatively solve a larger percentage of initially unsolved crimes than during 1984 - 85.

Figures are shown in Table 6.25 relating to the successful investigating of crimes in 84 - 85 versus 85-86. The numbers of crimes listed reflect those in which a suspect was not identified at the time the initial report was taken, and for which follow-up investigation was warranted.

TABLE 6.25
INVESTIGATIVELY SOLVED CRIMES

Year	Number of Crimes	Number Solved	%
84-85	232	8	3.44
85-86	124	11	8.87

In both time periods, the investigations almost exclusively dealt with either employee, visitor, or patient theft. While there was only a slight increase in the actual numbers of crimes solved investigatively in 85 - 86, it represented a considerable increase in terms of the overall percentage as opposed to 84 - 85 (i.e., almost 9 percent versus slightly over 3 percent). In each case, the

perpetrator, who was identified, was either discharged or prosecuted.

This objective was met.

13.2: To investigatively identify all unsafe conditions and practices which contributed to the occurrence of crimes and to present specific, corrective recommendations for preventing their recurrences.

The new security program had been sufficiently "debugged" during 84 - 85, so that few unsafe conditions remained. Most of the problems in 85 - 86 related to the personal practices of individuals (e.g., carelessness or ignorance). Nevertheless every crime was analyzed for its underlying causes and contributing factors. Appropriate recommendations were then made.

This objective was met.

13.3: To ensure that all corrective recommendations for crimes . . . are fully implemented, once the appropriate approvals are received.

In every case where a recommendation for corrective action was adopted by the appropriate authorities, follow-up was made to ensure that it was indeed properly implemented. Direct assistance was provided by the security department as necessary. Once corrective measures were put into place there were no recurrences of the crimes which prompted their implementation.

This objective was met.

Summary. All three objectives were met, resulting in the goal being achieved. Therefore, Hypothesis 13 is accepted.

Hypothesis 14

Provision of those miscellaneous services required for the general welfare and efficient operations.

14.1: To provide the same range and amount of miscellaneous "helping" services and general assistance to the institution as during 1984-85.

Due to the "limited" scope of services provided by the security department before the reorganization, as well as poor record-keeping, meaningful quantitative comparisons between 83 - 84 and 84 - 85 could not be made. However, this can be done for the 84 - 85 versus 85 - 86 periods.

In Table 6.26 contained some of the more significant miscellaneous services provided by the reorganized department over the two time periods.

Overall, the department increased the level of miscellaneous services provided to the institution by over 24 percent in 85 - 86 as opposed to 84 - 85. In only two categories were there decreases. Patient Valuables Pick-ups were down because the patient population itself actually decreased. Motorist assists were down, largely because of a change in the department policy where security personnel were no longer permitted to do such things as change a vehicle's flat tire. (It was too time consuming and kept the person "off patrol" too long.) In all other categories, the amount of services rendered actually increased.

TABLE 6.26
MISCELLANEOUS SERVICES PROVIDED

	84-85	85-86	%(+/-)
Patient Valuables Pick-ups	808	659	- 18.4
Cash Escorts	92	622	+530.0
Patient Restraints	260	357	+ 37.3
Motorist Assists	787	479	- 39.1
Person Transports	768	1,201	+ 56.6
Property Transports	370	528	+ 42.7
Morgue Assists	436	474	+ 8.7
Door Locks/Unlocks	6,054	8,001	+ 32.2
Employee/Visitor Escorts	4,852	5,602	+ 15.5
	14,427	17,923	+ 24.2

It should be noted that a number of these services were not even provided before the reorganization (i.e., in 83-84). These included cash escorts, patient valuables pick-ups, and door locks/unlocks. The reason for this was that security personnel then weren't trusted with these tasks.

This objective was met.

14.2: To provide inservice training to health center staff in the following areas.

Physical Management of "Disturbed" Persons
Fire Protection
Tornado Protection
Patient Relations
C.P.R.
Patient Searches

This objective was met.

14.3: To provide to health center staff the following loss prevention services for personal use:

Operation I.D.
Vehicle Etching
Security, Safety and Fire Protection Pamphlets
Child Fingerprinting and Identification

This objective was met.

14.4: To provide the surrounding community the following loss prevention services:

Child Protection Training
Child Fingerprinting and Identification
X-raying Halloween Candy

This objective was met.

14.5: To administer and maintain the following loss prevention programs:

Access and Parking Control
Key Control
I.D. Badge
Vehicle Registration
Property Removal Pass
Operation I.D. of Health Center Property
Lost and Found
Patient/Visitor/Employee Search

This objective was met.

14.6: To provide active participation in the following community-wide crime prevention programs and activities associated with Warren/Conner Coalition:

"Youth On Edge"
"Anticrime Task Force"
"Copes and Neighbors"
"Neighborhood Security Patrol"

This objective was met.

14.7: To upgrade, revise, and implement the "New Employee Orientation" program on security . . .

This objective was met.

14.8: To develop and implement a televised patient security program as part of the institution's patient education program.

This objective was still not met.

14.9: To develop and provide a "Security/Safety Fair"" for health center employees.

This objective was met.

Summary. Eight of the nine objectives were met. Only the objective to develop a patient television program was still not accomplished. Overall, however, the goal was achieved. Therefore, Hypothesis 14 is accepted.

Hypothesis 15

The effective acquisition, development, and maintenance of all departmental resources.

15.1: To maintain at all times a manpower pool of qualified job applicants in each job classification.

This objective was met.

15.2: To maintain "standing" manpower levels at all times which satisfy the institution's routine staffing needs.

This objective was met.

15.3: To hire qualified applicants on the basis of a fair and effective selection process.

This objective was met.

15.4: To promote qualified employees on the basis of a fair and effective promotional process.

This objective was met.

15.5: To provide active recruitment, selection, and promotion of qualified applicants in accordance with all applicable civil rights legislation.

This objective was met. (No successful challenges were ever made by unselected minority applicants.)

15.6: To maintain a racial and sexual composition of department members which reflects that of the community and the institution.

This objective was met. (The racial and sexual composition remained about the same as in 84 - 85.)

15.7: To review, revise, and utilize the department policy and procedure manual, which describes all job duties and expectations for all job classifications.

This objective was met.

15.8: To review, revise, and conduct an effective basic training program for all employees which consists of no less than 80 hours of formal classroom and O.J.T. instruction and also includes both written and practical application examinations.

This objective was met.

15.9: To review, revise, and conduct an effective advanced training program for "sworn" employees which consists of no less than 230 hours of formal classroom and field instruction and also includes both written and practical application examinations.

This objective was met.

15.10: To develop and conduct an annual maintenance training program for all employees, which consists of 80 hours of formal instruction for "sworn" personnel and 40 hours for nonsworn personnel.

This objective was met.

15.11: To provide additional job-specific training for all employees on an "as needed" basis.

This objective was met.

15.12: To develop, maintain, and utilize a video library of relevant training materials.

This objective was met.

15.13: To develop and implement a "Field Training Officer" program for new employees.

This was a new objective which involved a formal on-the-job training program for new security personnel under the supervision of assigned training Specialists. It was

primarily developed but not implemented by the end of the 85 - 86 period.

This objective was not met.

15.14: To provide supervisory and management personnel with additional "professional development" training opportunities.

This objective was met.

15.15: To provide interested personnel with additional training for the purpose of becoming inhouse instructors.

This objective was met.

15.16: To maintain the institution's computerized security system in good working order at all times.

This objective was met.

15.17: To maintain all department issued hardware and equipment in good working order at all times.

This objective was met.

15.18: To maintain accurate, up-to-date department records at all times.

This objective was met.

Summary. Seventeen of the 18 objectives were met, resulting in the goal being achieved. Therefore, Hypothesis 15 is accepted.

Hypothesis 16

The effective utilization and management of all existing departmental resources.

16.1: To maintain adequate shift overage and duty assignments at all times, according to the institution's needs.

This objective was met.

16.2: To identify changing institutional needs as they emerge and provide both adequate resources and effective procedural responses to them.

This objective was met.

16.3: To adhere to all applicable laws, policies, procedures, rules and regulations pertaining to the management and utilization of department resources at all times.

This objective was met.

16.4: To give time-off, assign, supervise, discipline and reward personnel in a fair and equitable manner at all times.

This objective was met.

16.5: To provide performance planning assistance to all personnel and administer performance appraisals on a semi-annual basis.

This objective was met.

16.6: To develop and utilize a managerial performance planning/appraisal system utilizing the M.B.O. approach.

This objective was met.

16.7: To satisfactorily pass all external and internal audits/inspections pertaining to department operations, effectiveness, and management.

The department was reviewed again by an outside consulting firm, once more by the Michigan State Police, and finally, by the hospital administration. No deficiencies were noted by any of these groups.

This objective was met.

16.8: To thoroughly investigate all complaints and concerns made about the department and take appropriate remedial action in a timely fashion.

This objective was met.

Summary. All eight objectives were met resulting in the goal being achieved. Therefore, Hypothesis 16 is accepted.

Hypothesis 17

Adherence to fiscal constraints on departmental resources in a cost-efficient manner.

17.1: To operate within approved budgetary allocations for the year.

This objective was met.

17.2: To formulate and justify an annual budget request for the upcoming year which is accurate and satisfies the department's actual fiscal needs without unnecessary expense to the institution.

This objective was met.

17.3: To demonstrate cost-justification for all unanticipated expenses and overtime occurred.

This objective was met.

17.4: To reduce turnover rates below the previous year's level.

The only major problem encountered in 84 - 85 (after the reorganization) was in the turnover of departmental personnel. Several newly hired employees had to be discharged for either failing the training program or else violating the new policies and procedures of the department. In addition, a number of the new employees were laid-off Detroit Police Officers. Shortly after the reorganization took place, they were rehired by Detroit.

All told, 45 percent of the staff in the new security department resigned or were fired in 84 - 85. Fortunately, they were immediately replaced by equally qualified

candidates. In 85 - 86, the situation was stabilized and a turnover rate of only 12.5 percent was experienced. Only 5 employees quit or were fired in 85 - 86 versus 18 resignations and discharges in 84 - 85.

This objective was met.

17.5: To reduce absenteeism rates below the previous year's level.

In 84 - 85, there was a daily absenteeism rate of approximately 8 percent. While this was still lower than in 83 - 84 (i.e., 11 percent), further improvement was desired. Through a variety of incentives (both positive and negative), this figure was reduced in 85 - 86 to approximately 5 percent.

This objective was met.

17.6: To generate at least $35,000 in parking revenue for the institution during the year to partially offset department expenses.

This objective was met.

17.7: To develop and market a training program for other institutions to utilize for a fee to partially offset department expenses.

The department's extensive training program was successfully shared by the security personnel at a number of other institutions. For each participant, a nominal fee was paid. The revenue generated more than covered the training expenses for the departmental personnel themselves. As a result, the training was "free" to the hospital and a small profit was realized.

This objective was met.

Summary. All seven objectives were met, resulting in the goal being achieved. Therefore, Hypothesis 17 is accepted.

Hypothesis 18

A healthy organizational climate within the department which fosters positive working relationships and teamwork.

18.1: To maintain the department's favorable self-perceptions in terms of morale and performance, at 1984 - 85 levels.

The same survey questions asked in June 1985 were again presented to the department in June 1986. There were 37 out of 40 members of the department present when the questionnaire was administered and all of them responded.

TABLE 6.27
OVERALL SELF-PERCEPTIONS

	84-85			85-86			
	n	x	s	n	x	s	T-Value
Public Relations	33	3.73	.84	37	3.97	.90	-1.18
Crime Prevention	33	3.79	.82	37	4.35	.68	-3.15*
Investigative Skills	34	3.76	.89	36	3.83	.88	- .32
Crisis Intervention	33	4.36	.60	35	4.57	.60	-1.41
Communication Skills	34	4.00	.78	37	4.08	.83	- .42
Job Knowledge	34	4.00	.70	37	4.19	.70	-1.14
Dedication/Interest	33	3.73	.84	37	3.86	.86	- .68
Professional Demeanor	33	3.97	.73	35	3.97	.79	- .01
Response Time	33	4.64	.74	37	4.62	.64	.09
Miscellaneous Services	33	4.18	.81	37	4.35	.68	- .96
Fire Prevention/Control	34	3.91	.87	37	4.46	.65	-3.03*
Safety	34	4.18	.67	36	4.33	.68	- .97
Overall Image	33	4.24	.61	37	4.22	.75	.16
Overall Performance	31	4.19	.65	37	4.27	.69	- .47

*Significant at $\alpha = .05$

$\bar{x}$		INTERPRETATION
0.0 to 1.49	=	Poor
1.5 to 2.49	=	Needs Improvement
2.5 to 3.49	=	Adequate
3.5 to 4.49	=	Good
4.5 to 5.0	=	Excellent

In Table 6.27 it is shown how the security department members evaluated themselves in 85 - 86 versus 84 - 85 (on a 1 - 5 point Likert scale). Two additional categories are included from similar 83 - 84 versus 84 - 85 comparisons. They are Fire Prevention and Control as well as Safety. They reflect additional areas of responsibility for the security program as part of its expanded role after the reorganization.

The department was generally consistent in its self-perceptions over both time periods. It still rated itself as "Good" in every category, except for Crisis Intervention and Response Time where it was "Excellent." In two categories, Crime Prevention and Fire Prevention and Control, the department indicated a significant improvement in performance. All other areas were rated at least as good as in 84 - 85.

Overall departmental morale was also assessed again (on a 1 - 10 scale) and compared to 84 - 85. The results are shown in Table 6.28.

TABLE 6.28
DEPARTMENT MORALE

84-85			85-86			T-Value
n	x	s	n	x	s	
30	7.33	1.40	34	7.56	.99	-.75

There was no significant difference in overall morale between the two time periods. It basically remained constant.

The department's overall satisfaction with the quality of the services it provided are shown in Table 6.29.

TABLE 6.29
SATISFACTION WITH QUALITY OF SERVICES

	84-85		85-86	
	n	%	n	%
Almost Always Satisfied	19	55	20	56
Generally Satisfied	14	41	15	42
Generally Dissatisfied	0	0	1	3
Almost Always Dissatisfied	1	3	0	0

Percentages for 85 - 86 do not equal 100 percent due to rounding error.

There was virtually no difference in satisfaction levels between the two time periods. The person who had indicated that he was almost always dissatisfied in 84 - 85 softened his position somewhat in 85 - 86. The remainder of the respondents were consistent in their overall satisfaction levels. Over one-half were "Almost Always Satisfied" with the quality of services provided.

The respondents' opinions are shown in Table 6.30 on how well the department compared overall in 85 - 86 as opposed to 84 - 85 (i.e., the second year of the reorganization versus the first year).

TABLE 6.30
OVERALL COMPARISON TO PREVIOUS YEAR

	n	%
Much Improved	14	39
Slightly Improved	17	47
About the Same	3	8
Slightly Worse	1	3
Much Worse	0	0
Don't Know	1	3

The general consensus of the respondents was that the department had continued to improve from the first year after the reorganization. One new employee didn't know and another one expressed a negative view (the same person who was dissatisfied on the other questions). Three felt the department was the same, but 86 percent noted some level of improvement.

A comparison is shown in Table 6.31 of how the department was rated in terms of the respondents' original expectations at the new location.

TABLE 6.31
EXPECTATIONS OF THE DEPARTMENT

	84-85		85-86	
	n	%	n	%
Greatly Exceeds Expectations	4	13	11	32
Somewhat Exceeds Expectations	17	53	13	38
Meets Expectations	10	31	8	24
Somewhat Fails to Meet Expectations	1	3	2	6
Greatly Fails to Meet Expectations	0	0	0	0

In spite of the fact that in 85 - 86 one additional person indicated the department failed to meet expectations, the general view was that it met them better. A considerably larger number of respondents in 85 - 86 stated that the department "Greatly Exceeds Expectations" than in 84 - 85 (i.e. 11 versus 4).

Another question dealing with the overall performance of the department (on a 1 - 10 scale) was asked for both time periods. The results are shown in Table 6.32.

TABLE 6.32
OVERALL PERFORMANCE

84-85			85-86			T-Value
n	x	s	n	x	s	
31	8.32	.98	36	8.56	1.08	- .92

There was no significant difference in either direction on the measure. In both 84 - 85 and 85 - 86 the respondents rated themselves quite favorably in terms of overall performance, but there was no meaningful change in opinions.

A final question was asked on whether or not the departmental personnel felt safe at work. Thirty-five out of 36 respondents indicated "Yes" (i.e., 97 percent). This compared to 100 percent of 33 respondents in 84 - 85. Practically speaking, however, the department overall was still not afraid of working in the environment of the new location.

On virtually every criterion of performance and morale, the department evaluated itself as well in 85 - 86 as in 84 -85 (in some cases better). Therefore, this objective was met.

18.2: To reach consensus on department related problems and their solutions via department-wide participation and collaboration in the "Questionnaire on Quality of Relationships in the Hospital" process.

This objective was met.

18.3: To positively reward overall performance by matching performance ratings with merit salary increases in a fair and equitable manner.

This objective was met.

18.4: To reward outstanding individual achievements via a department "awards" program.

A decision was made to take advantage of the already established and more prestigious awards programs available through the Detroit Police Department, Detroit Fire Department, and the American Red Cross. Members of the security department still received letters of commendation for valor and/or life saving. They were also "written up" in the hospital's biweekly newsletter. In addition, however, they were also recommended for an appropriate award from these public agencies. Five such awards were actually presented to departmental members in 85 - 86.

The intent of this objective was technically met.

Summary. All four objectives were met resulting in the goal being achieved. Therefore, Hypothesis 18 is accepted.

Hypothesis 19

A positive image of the department within the health center and community which promotes confidence, trust, cooperation, and favorable public relations.

19.1: To maintain the institution's favorable perception of the department in terms of its overall performance, image, and professionalism at 1984 - 85 levels.

When the attitudinal surveys were administered for 83-84 and 84 - 85, the entire total management team (i.e., administrators, department heads, managers, and supervisors) was included. Unfortunately, the author was not permitted by his supervisor to survey this entire sample group for the 85 - 86 period. Only administrators and department heads were allowed to be included. This resulted in a sample of only 27 respondents, as opposed to the 73 who responded in 1985.

The results of this smaller sample's views of the security department are shown in Table 6.33 and compared to the larger sample's views in the previous year. It pertains to the same 12 categories used previously. It also includes two additional categories, Fire Prevention and Control, and Safety.

The respondents' attitudes toward the department improved dramatically. Positive statistically significant differences were noted in every category except Crisis Intervention. The department was still rated as "Good" in all categories with the exception of Response Time,

Professional Demeanor, Overall Image, and Overall Performance where the ratings were "Excellent."

In Table 6.34 a comparison is made of how the respondents also rated the department in terms of overall performance (on a 1 - 10 scale) between 84 - 85 and 85 and 86. A significant improvement was noted here too.

TABLE 6.33
OVERALL EMPLOYEE PERCEPTIONS

	84-85			85-86			
	n	x	s	n	x	s	T-Value
Public Relations	69	3.72	.77	26	4.27	.87	-2.97*
Crime Prevention	69	3.68	.74	26	4.46	.65	-4.75*
Investigative Skills	60	3.63	.61	26	4.09	.68	-2.91*
Crisis Intervention	61	3.82	.79	22	4.18	1.00	-1.72
Communication Skills	69	3.80	.70	24	4.21	.66	-2.52*
Job Knowledge	67	4.04	.71	27	4.44	.64	-2.52*
Dedication/Interest	68	3.99	.64	27	4.44	.58	-3.26*
Professional Demeanor	71	4.10	.76	27	4.56	.51	-2.89*
Response Time	66	3.85	.90	26	4.50	.65	-3.36*
Miscellaneous Services	64	3.80	.74	23	4.35	.71	-3.09*
Fire Prevention/Control	64	3.77	.81	27	4.46	.59	-3.82*
Safety	66	3.74	.62	26	4.46	.58	-5.12*
Overall Image	72	3.92	.69	26	4.5	.58	-3.85*
Overall Performance	71	3.93	.54	26	4.5	.58	-4.49*

*Significant at $\alpha = .05$

$\bar{x}$		INTERPRETATION
0.0 to 1.49	=	Poor
1.5 to 2.49	=	Needs Improvement
2.5 to 3.49	=	Adequate
3.5 to 4.49	=	Good
4.5 to 5.0	=	Excellent

TABLE 6.34
OVERALL PERFORMANCE

84-85			85-86			T-Value
n	x	s	n	x	s	
68	7.96	1.13	24	8.79	.93	-3.26*

*Significant at $\alpha = .05$

In Table 6.35 another measure of overall employee satisfaction with the department is made.

TABLE 6.35
SATISFACTION WITH QUALITY OF SERVICES

	84-85		85-86	
	n	%	n	%
Almost Always Satisfied	34	47	23	85
Generally Satisfied	39	53	4	15
Generally Dissatisfied	0	0	0	0
Almost Always Dissatisfied	0	0	0	0

In both time periods, the respondents were at least generally satisfied with the quality of services provided by the department. However, the level of satisfaction increased markedly in 85 - 86. Eighty-five percent were almost always satisfied as opposed to only 47 percent in 84 - 85.

The administrators and department heads were also asked how the department compared overall in the second year after the reorganization as opposed to the first year. The results are shown in Table 6.36.

TABLE 6.36
OVERALL COMPARISON TO PREVIOUS YEAR

	n	%
Much Improved	4	18
Slightly Improved	11	50
About the Same	3	14
Slightly Worse	0	0
Much Worse	0	0
Don't Know	4	18

Four respondents were new employees and couldn't compare the department over the two year period. Of those who could, 68 percent felt it had improved to one degree or another. The remainder thought it was about the same.

Lastly, the respondents were asked to compare the department to other hospital security departments they had dealt with or been exposed to. Their responses are shown in Table 6.37.

TABLE 6.37
COMPARISON TO OTHER HOSPITAL SECURITY DEPARTMENTS

	84-85		85-86	
	n	%	n	%
Much Better	28	41	17	71
Slightly Better	14	21	6	25
About the Same	9	13	0	0
Slightly Worse	1	1	0	0
Much Worse	0	0	0	0
Don't Know	16	24	1	4

Only one respondent in 85 - 86 couldn't compare the department to others, as opposed to 16 in 84 - 85. The reason for this is that the respondents in 84 - 85 included

managers and supervisors. They had less experience in the health care field than the administrators and department heads in the 85 - 86 sample, who had worked at other hospitals during their career.

When comparing those who did voice an opinion, there was a noticeable shift in favor of the department. Even though 62 percent of the respondents in 84 - 85 felt the department was at least "Slightly Better" than other hospital security departments, 14 percent thought it was "About the Same" or "Slightly Worse." In 85 - 86 virtually everyone felt it was at least "Slightly Better." Seventy-one percent actually judged it as being "Much Better."

On every measure, the department was rated better by the respondents in 85 - 86 than in 84 - 85. Although the 85 - 86 sample group was considerably smaller than in 84 - 85, it represented the "top echelons" of the institution and was still considered representative of the general views of the entire hospital. Furthermore, no formal criticisms nor complaints were registered against the department by any of the general employee population during the entire 85 - 86 period. Informal feedback was always positive.

This objective was met.

19.2: To promote a general feeling of "personal safety" on the part of the institution's employee population.

In the January 1985 hospital-wide survey administered by the Personnel Department, one question addressed employee concerns about personal safety. (The results have already

been discussed for Objective 9.2.) Another hospital-wide survey was originally planned for 1986. It would have contained the same question. Unfortunately the entire survey was cancelled. Therefore no direct hospital-wide comparison can be made for this objective.

The only quantitative measure available for 85 - 86 comes from the survey administered to the administrators and department heads. Of the 25 respondents who answered the question on whether or not they felt safe at work, 100 percent indicated that they did indeed feel safe.

A couple of indirect (and admittedly subjective) measures of the overall employee opinions on personal safety can be discussed. First, no formal complaints nor concerns were ever voiced by any employee to the security department or administration during the entire 85 - 86 period. Second, there were informal monthly meetings held between the president of the hospital and employees. These were conducted for the expressed purpose of allowing employees to share concerns, make complaints, and engage in joint problem-solving. Personal safety and security were never brought up as issues at any of these meetings.

This objective was met.

19.3: To maintain positive working relationships with other segments of the institution, patients, visitors, and physicians with whom contact is made.

This objective was met.

19.4: To maintain positive working relationships with local criminal justice, fire, and community

agencies/organizations with whom contact is made.

This objective was met.

Summary. All four objectives were met resulting in the goal being achieved. Therefore, Hypothesis 19 is accepted.

Hypothesis 20

Effective communication links within the department, the health center, and the community.

20.1: To disseminate all information necessary for effective operations on a daily basis at shift briefings.

This objective was met.

20.2: To provide complete, up-to-date and timely instructions on all new or revised policies, procedures, rules, and regulations which pertain to department personnel.

This objective was met.

20.3: To conduct periodic department-wide meetings for the purpose of joint planning, problem-solving, information sharing.

This objective was met.

20.4: To conduct periodic "management team" meetings for the purpose of joint planning, problem-solving, information sharing, and coordinating of routine operations.

This objective was met.

20.5: To provide timely status reports to the appropriate authorities on department operations, individual incidents, emerging problems, and alternative solutions.

This objective was met.

20.6: To provide active participation on all assigned committees/task forces and at all relevant meetings conducted by the health center.

This objective was met.

20.7: To disseminate security . . . information and instructions to all affected personnel in the institution whenever necessary.

This objective was met.

Summary. All seven objectives were met, resulting in the goal being achieved. Therefore, Hypothesis 20 is accepted.

1985 - 86 Results

There are ten goals (i.e., general hypotheses) and 68 objectives for the 85 - 86 period. All of the goals are the same as those in 84 - 85. Most of the objectives are the same also, but there are a few more of them and some are even more ambitious than for 84 - 85. (This is particularly true for those objectives dealing with actual crime-related issues.) Twelve of them involve direct comparisons with 84 - 85.

The reorganized security program achieved even better results in its second year than in its first. Crimes continued to decline. The security department displayed an increased ability to effectively deal with them when they did occur. More miscellaneous services were provided to the hospital. The department's own self-perceptions and morale were maintained at acceptable levels. The positive opinions of the department by other employees was enhanced even further. They continued to feel safe at work.

All ten goals were achieved and 66 of the 68 objectives were met. Out of a possible total of 88 points for overall effectiveness, the program received 85, resulting in a 96.6 percent effectiveness rating. This was virtually the same

score as in 84 - 85, even though the program's objectives were sometimes more demanding.

CHAPTER SUMMARY

There are a total of 20 goals and 127 objectives which have been addressed in this chapter. The goals represent the functional equivalent of formal hypotheses and the objectives constitute their operationalized elements. One-hundred twenty-three of those objectives were satisfied and all 20 goals were achieved. This is tantamount to stating in a more traditional type of research study that all of the hypotheses have been accepted.

The reorganized security program was examined from a variety of perspectives. However, perhaps the most important overall measure of any security program is the degree to which it can prevent and actually reduce crime. The effectiveness of the program in this regard can be summed up and visually illustrated with a series of simple figures.

In Figure 6.1 a comparison is made of the overall number of major (i.e., Part I) crimes committed over the three year period of the study. These crimes include homicide, robbery, criminal sexual conduct, breaking-and-entering, auto theft, felonious assault, arson, and larceny over $100. In Figure 6.2 just auto thefts are compared. In Figure 6.3 just larcenies over $100 are compared. In Figure 6.4 the total economic impact from all reported crimes is compared.

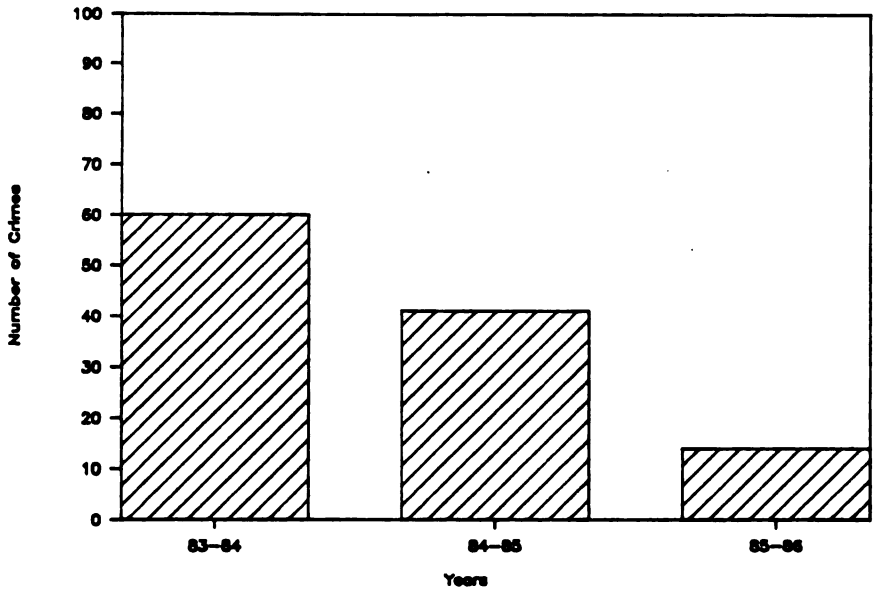


FIGURE 6.1
MAJOR CRIMES

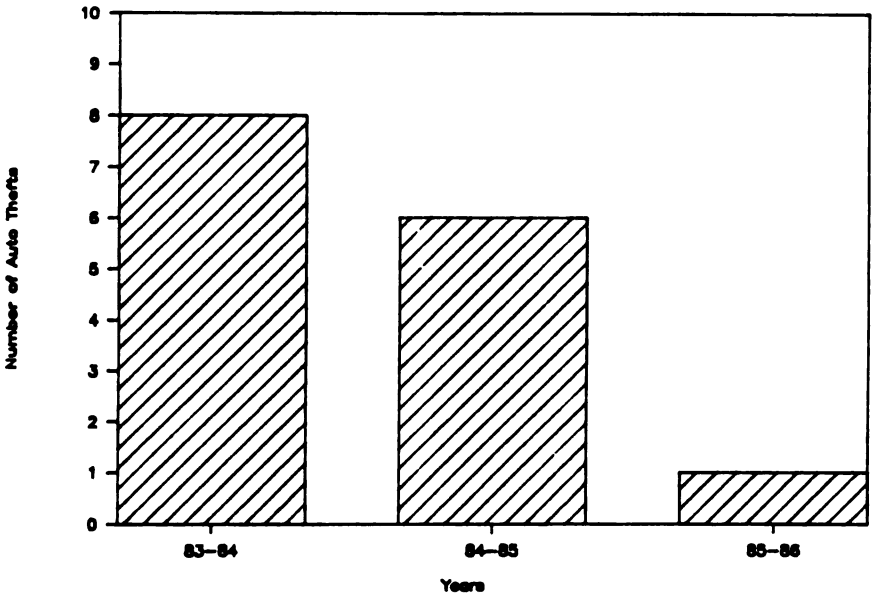


FIGURE 6.2
AUTO THEFTS

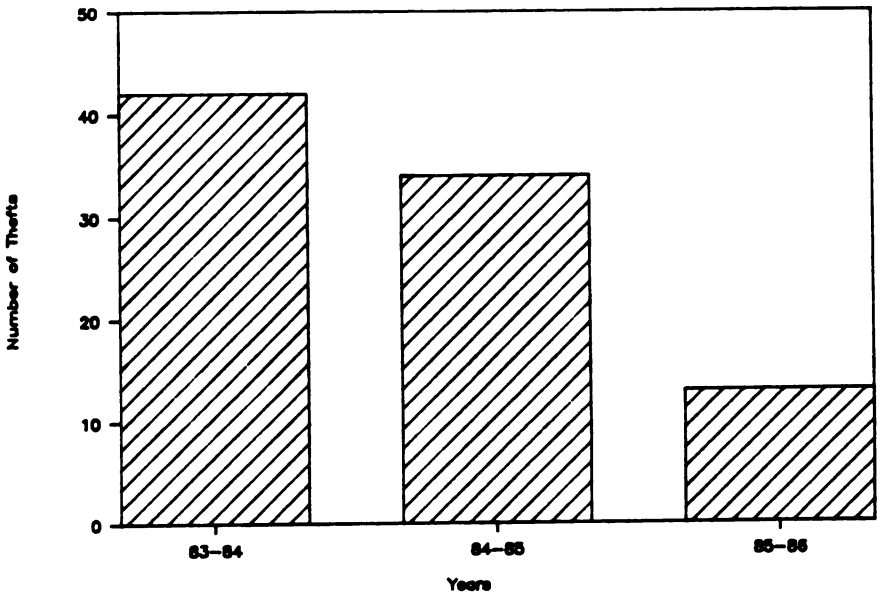


FIGURE 6.3
LARCENIES OVER $100

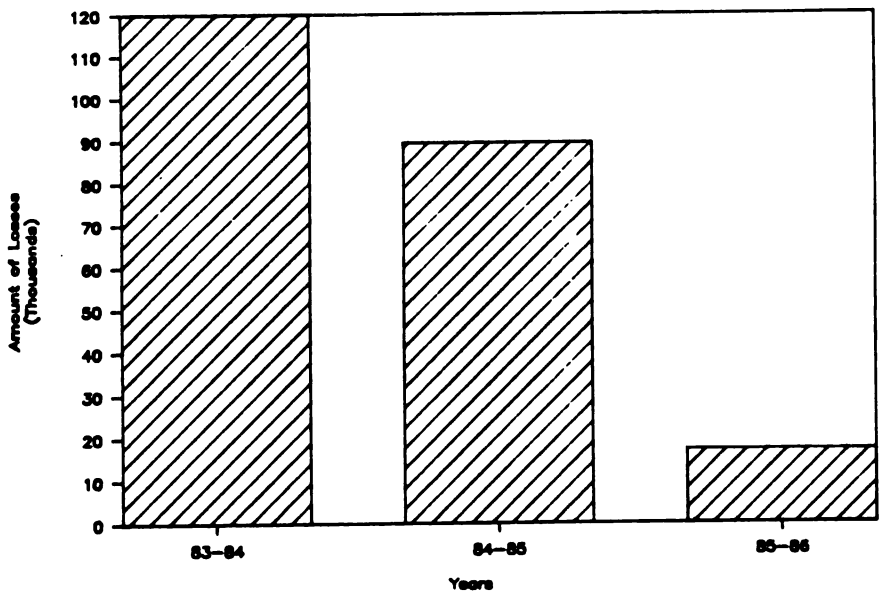


FIGURE 6.4
MONETARY VALUE OF LOSSES

All four figures reveal a definite downward pattern in crime levels. Unfortunately, due to poor reporting and record-keeping during the 83 - 84 period direct comparisons of all crimes (including misdemeanors and larcenies under $100) are not possible over all three years. However, for 84 - 85 and 85 - 86 complete data are available. In Figure 6.5 the trend in all crimes by month from 84 to 86 is demonstrated. In Figure 6.6 the trend in all larcenies for the same 24-month period is also shown.

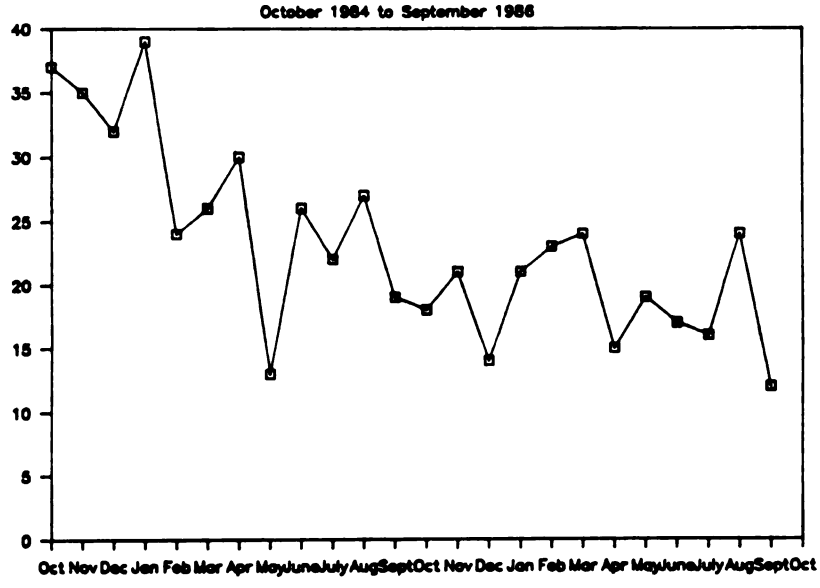


FIGURE 6.5
ALL CRIMES

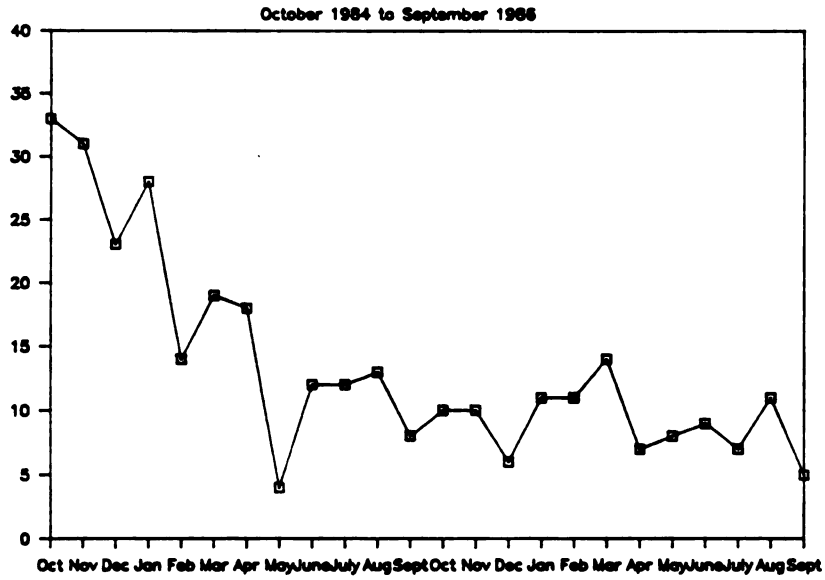


FIGURE 6.6
ALL LARCENIES

Both figures reveal a relatively stable downward trend. The first few months were the worst. However, after all the security hardware was installed and other elements of the new program "debugged" the crime rate steadily decreased.

Even without the wide variety of other analyses conducted, these six figures alone provide convincing evidence of how successful the reorganized security program had become.

There is one final measure which hasn't been discussed yet. This is because it wasn't one of the original Goals and Objectives. However, it may actually be the most significant single criterion of all, namely, professional recognition.

At the end of the 85 - 86 period, the reorganized security program earned the two most prestigious awards in the field. First, it won the award for the "Outstanding Crime Prevention Program" in the State of Michigan. Second, it won the award for the "Outstanding Hospital Security Program" internationally. These awards were given by the Crime Prevention Association of Michigan and the International Association for Hospital Security, respectively. In effect, these two professional groups recognized the security department as being the best of its kind.

CHAPTER 7

SUMMARY AND CONCLUSIONS

SUMMARY

Purpose

In one sense this study represents a straightforward program evaluation, an example of Action Research. Samaritan Health Center, a Detroit based community hospital, built a new facility which was located in an extremely high-crime area. The employee population was very concerned about moving to the new location, especially since the existing security program was generally viewed as inadequate. As a result an administrative decision was made to reorganize that program to better protect the new environment.

To a larger degree this study also constitutes a field test of a theoretical framework for managing security programs in general. Comprehensive models for the development, implementation, and evaluation of security programs were generally lacking in the field. Therefore, one was developed to be a "blueprint" for the creation of the reorganized program at Samaritan. It was designed to be specific enough for the particular needs of the institution and generic enough to be applicable to the security field in general.

Theoretical Framework

The theoretical framework upon which the new security program was developed consists of several separate models, techniques, and approaches. They are all integrated and complementary. Some portions have been developed by the author and some compiled from the works of others.

At the heart of this framework is the ACTION MODEL. This is the basic strategy for conducting a security program. It identifies the major responsibilities of management as the cyclical processes of Evaluation, Planning, and Execution. For each one of these processes there are several discreet tasks, which must be performed to accomplish them. Accompanying these tasks are components which in effect are operational tools or skills needed to complete the tasks.

A necessary supplement to the ACTION MODEL is some type of general systems perspective of the problems and solutions associated with a security program. Therefore, an applied Systems View model is included, which identifies two basic dimensions for analyzing those problems and solutions. One deals with the security system components of People, Property, and Practices. The other deals with social system levels from the Individual to the entire Environment. A third dimension is also sometimes appropriate, namely, time frames relative to the potential occurrence of a crime (i.e., Before, During and After).

The overall framework also contains several other supporting components. First, a Management-by-Objectives approach is employed which identifies specific Goals and Objectives to be achieved and helps to structure the activities associated with them. Second, a basic Decision-making and Problem-solving scheme is also provided to assist in individual cognitive processes. Finally, an elaborate set of strategies for Implementing Change is incorporated to facilitate the approval of and support for plans that are ultimately developed. These identify sources of resistance, reasons for it, and methods for overcoming it.

Method

The procedures for directly evaluating the reorganized security program (and indirectly the theoretical framework itself) were developed to be as methodologically sound as possible, given "real world" limitations and realities.

The hypotheses were admittedly somewhat unconventional. They reflected the M.B.O. goals and objectives set for the reorganized program. The general hypotheses were goals; their operational definitions were objectives. There were a total of 20 general hypotheses and 127 operational definitions for them. They were organized in two sets, one for the 84 - 85 period based on ten goals and 59 objectives, and one for the 85 - 86 period based on ten goals and 68 objectives. Some objectives were quantitative in nature and some non-quantitative.

The research design, by necessity, was not truly "experimental." However, a pretest-posttest-posttest design was employed for most of the quantitative objectives. Where pretest data was not available a posttest-posttest design was utilized. The pretest reflected the October 1983 to September 1984 time period, immediately preceding the reorganization. Posttest 1 reflected the October 1984 to September 1985 time period, the first year after the reorganization. Posttest 2 reflected the October 1984 to September 1985 time period, the second year after the reorganization.

The quantitative data were basically of two types. The first included compiled statistics relating to crimes, security-related incidents, and miscellaneous services rendered. The second consisted of attitudinal measures relating to the security program. Data collection for the former was based on formal incident reports written by security personnel, as well as daily activity records. Data collection for the latter is based on formal survey instruments administered to employees.

The survey instruments consisted of a variety of questions formatted as either multiple choice, open-ended, Likert type (i.e., 1 - 5 scales or 1 - 10) scales. They addressed a number of perceptions about the overall quality of the security program.

The survey subjects included members of the security department as well as a stratified sample of the remainder

of the hospital population. This latter sample consisted of administrators, department heads (including physicians), managers, and supervisors in 83 - 84 and 84 - 85. Only administrators and department heads were included in the 85 - 86 sample.

The response rates for both sample groups were as follows. For the security department there were 14 respondents out of 36 members (i.e., 39 percent) for 83-84, 34 out of 40 (i.e., 85 percent) for 84 - 85 and 37 out of 40 (i.e., 93 percent) for 85 - 86. For the hospital total management team sample there were 105 respondents out of 172 members (i.e., 61 percent) for 83 - 84, 73 out of 138 (i.e., 53 percent) for 84 - 85, and 27 out of 42 (i.e., 64 percent) for 85 - 86.

Analysis was handled in two different ways. Non-quantitative objectives were evaluated subjectively by a panel of hospital administrators. They simply decided whether or not a particular objective had been met based on observation. Where quantitative objectives and data were involved, frequency tables, distributions, and percentages were calculated and compared, and (for scaled data) Two-Tailed T-Tests were conducted of the differences of means.

A hypothesis (i.e. goal) was either accepted or rejected on the basis of whether or not its accompanying objectives were met as determined by either quantitative or non-quantitative analysis. At least 75 percent of a goal's objectives had to be met in order for it to be considered

achieved (thereby equating to the acceptance of the hypothesis).

Findings

On virtually every quantitative measure comparing 83-84 to 84 - 85 (i.e., pretest vs. posttest) the analyses revealed improvements in the security program. "Negative" statistics such as numbers of crimes and related losses decreased. "Positive" statistics such as recovery rates and apprehensions increased. The department's own self-perceptions increased as did the views of the total management team sample toward the department. On every variable for which a T-Test was conducted a statistically significant positive difference was found. Furthermore, all but two of the non-quantitative objectives were determined to have been met.

The 84 - 85 to 85 - 86 (i.e., posttest 1 vs posttest 2) comparisons revealed even better results. "Negative" statistics continued to decline, while "positive" statistics continued to climb for virtually every variable analyzed. The department's own self-perceptions either maintained at or else improved over 84 - 85 levels. The management sample's opinions of the department continued to consistently improve. On all but two variables for which T-Tests were conducted, positive statistically significant differences were noted over even 84 - 85 levels. Again all but two of the non-quantitative objectives were met.

In summary all 20 hypotheses were accepted. One-hundred twenty-three of the 127 operational objectives were met, including every one subject to quantitative analysis. The security program's overall effectiveness rating, based on the percentage of objectives met, was 96.1 percent in 84 - 85 and 96.6 percent in 85 - 86.

CONCLUSIONS

Based on the results of the analyses, it can only be concluded that the reorganized security program by far surpassed its predecessor and was a complete success. This conclusion was reinforced by the awards received by the security department from professional organizations. Furthermore, it came to be known as a "Model" program in the field. Several hospital security managers visited the hospital to study the program, and six other hospital security departments actually emulated its law enforcement component. In addition, the author was asked by one hospital to develop a similar program at that institution under a management contract.

Since the reorganized program was developed, implemented, and evaluated completely within the context of the theoretical framework described in Chapter 3, it can be safely inferred that this overall model had considerable utility. For purposes of this study, it proved to be a very effective management tool and "passed" its first field test.

LIMITATIONS

In spite of the positive results obtained, the study itself had several potential limitations for which it could be criticized. Some of them are discussed below.

Design

In terms of the survey component of the study a quasi-experimental one-group pretest-posttest design was employed. Admittedly, it has limited ability to control against threats to internal and external validity. A better design would have been a one-group time-series design with multiple measurements being taken more periodically than once a year. This was not possible because of the hospital administration's reluctance to saturate the employee population with surveys. However, the second posttest incorporated into the study attempted to serve as somewhat of a compromise in this regard.

Sampling

Two limitations were present in sampling. First it was one-group and stratified in the sense that only management personnel were included. Second the sample size was small in comparison to the overall employee population. Ideally the entire population should have been surveyed or at least a larger, randomized sample should have been employed. Again, however, this was not possible due to constraints imposed by administration. Unfortunately, the primary concern was more with the opinions of the total management team than with the employee population as a whole. Hence

the survey findings cannot be generalized with confidence to everyone who worked at the hospital.

The issue of sampling the security department itself was not a problem because everyone was included. The only potential limitation here was in the poor response rate to the surveys in 83 - 84 (i.e. 39 percent).

Data Collection

An accurate and comprehensive data base of incident and miscellaneous services statistics was developed and maintained in both 84 - 85 and 85 - 86. However, this was not the case in 83 - 84. Statistics were not categorized in any consistent fashion. Few were even routinely kept. Therefore, some pretest-posttest comparisons were impossible (e.g., miscellaneous services provided). Others were not as accurate as they could have been (e.g., larcenies over $100). This did not invalidate the findings reached, but in many cases reduced the magnitude of the observed differences from what the actual differences probably were.

Survey Instrumentation

The survey questionnaire administered solely to department personnel was primarily used for diagnostic purposes and internal consumption. However, the question on morale was factored into the analysis of the study. All of the questions on the second questionnaire, which was administered to both sample groups, became part of the analysis.

Even though the surveys were informally pretested on a small scale, no formal tests were made. Therefore, a question could be raised about their reliability. However, the questions were formatted according to widely accepted methods and instructions were provided to all respondents. Terms were defined to eliminate uncertainties or ambiguities. Therefore, it is believed that reliability was not a problem.

Analysis

A potential criticism could be made about the way that a large number of non-quantitative objectives were evaluated subjectively by a panel of administrators. However, this was not necessarily a shortcoming. Some objectives were simply not amenable to quantification.

The panel was employed to consider a number of opinions, and obtain a consensual view, as opposed to merely one person's judgement. This hopefully improved the reliability of the assessments made.

External Validity

The overall degree of success of the security program at Samaritan Health Center can be directly attributed to the theoretical framework upon which it was developed, implemented, and evaluated. Still it cannot be predicted with certainty that the same results would be obtained in other institutions or organizations using the same methods.

Every institution has its own fairly unique set of problems, capabilities, and constraints. Therefore, the

generalizability of the theoretical framework must be viewed with some caution, especially on the basis of only one study. Nevertheless, its principles are sound and should possess some degree of universality.

DISCUSSION

Traditionally, it has been the norm in the hospital security field to just maintain the status quo and avoid "rocking the boat" if at all possible. Many security programs lack a clear sense of direction or well-defined goals. Emphasis is placed on merely coping with day-to-day problems and occurrences. The results are akin to always "catching up" instead of "getting ahead" in terms of providing a safe and secure hospital environment.

Part of this problem is because many security managers view their primary role as one of only managing. They fail to either understand or appreciate the need for and value of comprehensive program planning and evaluation. Plans that are made usually are short-term and problem-focused in nature. Evaluations are often limited to information requested by superiors or simple analyses of security-related statistics and budget reports.

Even those managers with a more enlightened perspective often have difficulty achieving desired results, because they lack the appropriate management tools to assist them. There simply haven't been any truly comprehensive program models available in the security field.

The primary contribution of this study is that it presents a comprehensive theoretical framework within which to conduct a hospital security program. As shown by the results, it was highly effective at Samaritan Health Center. Further applications at other institutions would be necessary to validate its ultimate utility. However, it still represents an advancement in the field of hospital security management, from which other security programs might well benefit.

Even if the theoretical framework was not to be further field tested and/or adopted by other security programs, there are a number of practical lessons which can be learned from the Samaritan experience. Several of the most significant ones are presented below in the form of recommendations, which are generally applicable to all programs, but frequently overlooked.

1) Establish clearly defined goals, which are feasible to attain.

It is not sufficient merely to state that a security program's overall goals are "to fight crime" or "to keep people safe." By themselves these phrases do not really say much, and are difficult to measure. More specific end-results are necessary to focus the program's direction and efforts. They should be formalized and communicated to both security personnel and the rest of the institution, so everyone knows what is to be expected from the security

program. Furthermore, they must be attainable and not beyond the means of the program to achieve.

2) Maintain an accurate updated data base, which can be used to measure the achievement of goals.

Not everything a security department does can be measured quantitatively. However, basic security-related statistics can be collected and maintained. They should be developed into standardized categories, recorded daily, and tabulated periodically (e.g., monthly). The types of data collected may vary from program to program, depending on the scope of services provided. However, they should be as comprehensive as possible and directly relevant to the overall goals set for the program.

3) Develop long-term plans for the program and follow them.

Annual operating plans should be established at a minimum. (Generally it is best to have them coincide with the hospital's budget cycle.) Shorter or longer-range plans may also be appropriate. The plans should define basic strategies aimed at achieving the program's goals. While it might become necessary to alter or modify individual plans, they should not be ignored once they are developed. All efforts and activities of the security program should be carried out within the context of those plans.

4) Establish and maintain a broad base of support for the plans.

<u>Formal</u> approvals and support for a security program's plans should be solicited before their implementation.

Ordinarily this would involve the security manager's own supervisor and perhaps the hospital administration as a whole. However, it is often equally important to obtain informal support. Since most plans are actually carried out by the members of the security department, they should develop some level of commitment to them. Furthermore, the employee population in general should at least be receptive to the plans, if not entirely supportive of them. Otherwise, lack of cooperation or even outright resistance might make the plans impossible to carry out successfully.

5) Remember that program management is a series of multi-faceted, on-going processes.

A security manager must not get "lost" in routine day-to-day activities and lose sight of planning and evaluation priorities. Neither should a manager just develop a plan, put it into motion, and then sit back to wait for the results. Effective management requires continual attention to all three cyclical processes of Evaluating, Planning, and Executing.

6) Don't lose sight of the "big picture."

Generally speaking crime is a complex problem. Simple short-term solutions are often inadequate. The underlying causes and causal relationships of crime should always be considered. Furthermore, a security program cannot pretend to operate in a vacuum. It is part of a larger social system called a hospital. The potential social ramifications of proposed security measures should always be

considered. On the other hand this same social system can also be mobilized to enhance the effectiveness of those measures, if done properly.

APPENDICES

APPENDIX A

ROUTINE DEPARTMENT STATISTICS: MONTHLY SUMMARY FORM

Samaritan Health Center
Department of Protective Services
Monthly Theft Summary

_____
MONTH

DATE	SHIFT	VICTIM	ITEM(S)	VALUE	RECOVERED

TOTALS: _____ NO. THEFTS _____ VALUE _____ NO. RECOVERED _____ VALUE RECOVERED

YTD TOTALS: _____ NO. THEFTS _____ VALUE _____ NO. RECOVERED _____ VALUE RECOVERED

PCI TOTALS: _____ NO. THEFTS _____ VALUE _____ NO. RECOVERED _____ VALUE RECOVERED

PCI YTD TOTALS : _____ NO. THEFTS _____ VALUE _____ NO. RECOVERED _____ VALUE RECOVERED

Samaritan Health Center
Department of Protective Services
Monthly Activity Summary

TIME PERIOD

CATEGORY							
CRIMES:							
Homicide							
Felonious Assault							
Aggravated Assault							
Assault & Battery							
Resisting & Obstructing							
Other Assaults							
Robbery Armed							
Robbery Unarmed							
Attempted Robbery							
CSC-Felony							
CSC-Misdemeanor							
Indecent Exposure							
Gross Indecency							
Other Sexual Conduct							
Carrying Concealed Weapon							
Discharging Firearm							
Other Weapon							
Disorderly Person							
Disturbance in Business							
Trespassing							
Unauthorized Entry							
Other Disorderly							
B & E - Building							
B & E - Vehicle							
Attempted B & E							
Other B & E							
UDAA							
Joy Riding							
Attempted UDAA							
Larceny - From Person							
Larceny - From Building							
Larceny - From Vehicle							
Larceny - From Machine							
Larceny - By Conversion							
Larceny - By Trick							
Larceny - Over $100							
Larceny - Under $100							
Defrauding Inn-Keeper							
Embezzlement							
Other Larceny							
R & C > $100							
R & C < $100							
MDOP> $100							
MDOP< $100							
C.C. - Intent to Circulate							
Other Credit Card							
Forgery							
Uttering & Publishing							

CATEGORY							
Counterfeit/Altered Money							
Non-Sufficient Funds							
No Account Checks							
Other Fraud							
Drugs - Sale							
Drugs - Use							
Drugs - Possession							
Other Drugs							
Abduction							
Arson							
Bomb Threat							
Extortion							
Child Neglect/Abuse							
False Police Report							
Impersonating Police Officer							
Gambling							
Obscene/Harassing Phone Call							
Threats							
Warrant Arrest							
Other Crimes							
TOTAL							
ARRESTS--TOTAL							
NON-CUSTODY PROS. TOTAL							
SECURITY:							
Disorderly Person-Advised Only							
Trespassing - Advised Only							
"Crisis" Intervention							
Civil Dispute							
Suspicious Person							
Suspicious Incident							
Suspicious Vehicle							
Security Hazard - Condition							
Security Hazard - Behavior							
Security Status Check							
Security Alarm Response-Unfounded							
Patient Valuables Pick-up							
Cash Escort							
Unsecured Door/Window/Area							
Equipment/Alarm Test/Inspection							
Special Detail							
Other							
Total							
SAFETY:							
Patient Restraint							
Careless/Reckless Driving							
Missing Person/Patient							
Safety Hazard - Condition							
Safety Hazard - Behavior							
Safety Status Check							
Accident-No Injury/Damage							
Accident-Property Damage							
Accident-Injury							
Health Emergency							

T.P. Patient Search							
Safety Alarm Response-Unfounded							
Equipment/Alarm Test/Inspection							
Traffic Accident-Damage							
Traffic Accident-Injury							
Special Detail							
Other							
Total							

FIRE:

Fire Hazard - Condition							
Fire Hazard - Behavior							
Fire/Smoke - No Damage							
Fire/Smoke - Property Damage							
Fire/Smoke - Injury							
Fire Drill							
Fire Alarm Response-Unfounded							
Equipment/Alarm Test/Inspection							
Special Detail							
Other							
Total							

EMERGENCIES:

Bomb Search							
Tornado/Thunderstorm							
Explosion							
Radiation Accident							
Hazardous Materials Accident							
Telephone Outage							
Power Failure							
Civil Disturbance							
Winter Storm							
External Disaster							
Emergency Preparedness Drill							
Special Detail							
Gas Leaks							
Other							
Total							

ASSISTS:

Assist Other Department							
Motorist Assist							
Person Transport							
Property Transport							
Morgue Assist							
Open/Close Door							
Light Left On							
"Emergency" Assist							
Special Detail							
General Citizen Assist							
Employee							
Visitor							
Patient							
Other							
Escorts							
Total							

MISCELLANEOUS:

- Alcohol On Premises
- Truancy
- Unauthorized Visiting
- Loitering
- Parking Violation
- Hospital Rules Violation
- Lost Property
- Found Property
- Property Damage - Unknown Cause
- Confiscated/Recovered Property
- Other
- Parking Tickets
- Total

OBSERVATION REPORTS:

- Security
- Safety
- Fire
- Administrative
- Maintenance
- Housekeeping
- Total

TOTAL DOCUMENTED ACTIVITIES:

INCIDENT REPORTS:

THEFTS:

Employee	#	
	$	
Visitor/Other	#	
	$	
Patient	#	
	$	
Hospital	#	
	$	
Total	#	
	$	

RECOVERED:

Employee	#	
	$	
Visitor/Other	#	
	$	
Patient	#	
	$	
Hospital	#	
	$	
Total	#	
	$	

APPENDIX B

ANNUAL DEPARTMENT PROGRESS SURVEY FORM

PROTECTIVE SERVICES

ANNUAL DEPARTMENT PROGRESS SURVEY

1. How would you rate the overall performance and leadership of Ellen Knight? (On a 1-10 scale) _____

2. How could she improve? _____

_____

_____

3. How would you rate the overall performance and leadership of Vanessa Jones? (On a 1-10 scale) _____

4. How could she improve? _____

_____

_____

5. How would you rate the overall performance and leadership of Ron Maksout? (On a 1-10 scale) _____

6. How could he improve? _____

_____

_____

7. How would you rate the overall performance and leadership of Marty Wahrer? (On a 1-10 scale) _____

8. How could he improve? _____

_____

_____

9. How would you rate the overall performance of your shift? (On a 1-10 Scale)

_____

10. How could your shift improve? _____

_____

_____

11. How would you rate the overall performance and leadership of Bruce Sokolove? (On a 1-10 scale) _____

12. How could Bruce improve? _____

_____

_____

13. How would you rate the overall performance and leadership of Robert Smith? (On a 1-10 Scale) _____

14. How could Smitty improve? _____

_____

_____

15. How does the overall performance of the entire department <u>today</u> compare with one year ago?

_____ BETTER

_____ SAME

_____ WORSE

_____ DON'T KNOW

16. How could the department improve? _____

_____

_____

17. How would you rate the overall morale of the department? (On a 1-10 Scale) _____

18. How could department morale be improved? _____

_____

_____

19. Additional comments/criticisms. _____

_____

_____

_____

THANK YOU!

APPENDIX C

HOSPITAL-WIDE OPINION SURVEY

SAMARITAN HEALTH CENTER
PROTECTIVE SERVICES OPINION SURVEY

In the interest of evaluating the quality of the Protective Services program at Samaritan Health Center, we would like your input and opinion as a consumer of our services. Please take a few moments to help us determine how well we're doing and where we can improve. Thank you for your cooperation.

Your Position:
(check one)

_____ Administrator
_____ Physician
_____ Department Head
_____ Manager
_____ Supervisor
_____ Other (Specify) _____

---

1) Please rate the Protective Services Department according to the following scale (check one for each item):

	Poor	Needs Improvement	Adequate	Good	Excellent
Public Relations	___	___	___	___	___
Crime Prevention	___	___	___	___	___
Fire Prevention & Control	___	___	___	___	___
Investigative Skills	___	___	___	___	___
Safety	___	___	___	___	___
Crisis Intervention (handling "disturbed" persons)	___	___	___	___	___
General Communication Skills	___	___	___	___	___
Job Knowledge	___	___	___	___	___
Dedication/Interest	___	___	___	___	___
Professional Demeanor	___	___	___	___	___
Response To Calls For Assistance	___	___	___	___	___
Miscellaneous Services Rendered	___	___	___	___	___
Overall Image	___	___	___	___	___
Overall Performance	___	___	___	___	___

2) What services should the Department be providing that it's not providing now?

_____

_____

_____

3) Overall how satisfied are you with the quality of services provided by the Department? (Check one)

_____ Almost Always Satisfied
_____ Generally Satisfied
_____ Generally Dissatisfied
_____ Almost Always Dissatisfied

4) Overall how does the Department compare <u>today</u> with a year ago? (Check one)

_____ Much Improved
_____ Slightly Improved
_____ About the Same
_____ Slightly Worse
_____ Much Worse
_____ Don't Know

5) Overall how does the Department compare with other hospital security departments you've seen or know about? (Check one)

_____ Much Better
_____ Slightly Better
_____ About the Same
_____ Slightly Worse
_____ Much Worse
_____ Don't Know

6) Overall how well does the Department rate in terms of your original expectations at our new facility? (Check one)

_____ Greatly Exceeds Expectations
_____ Somewhat Exceeds Expectations
_____ Meets Expectations
_____ Somewhat Fails to Meet Expectations
_____ Greatly Fails to Meet Expectations

7) <u>In general</u> do you feel safe at work? (Check one)

_____ Yes
_____ No

8) Based on your previous answers, please rate the overall performance of the Department on a one-to-ten scale (1=very poor and 10=excellent). _____

9) Please indicate any other suggestions, comments or constructive criticisms about the Department which may be helpful in improving our services to you.

_____

_____

_____

_____

_____

THANK YOU!

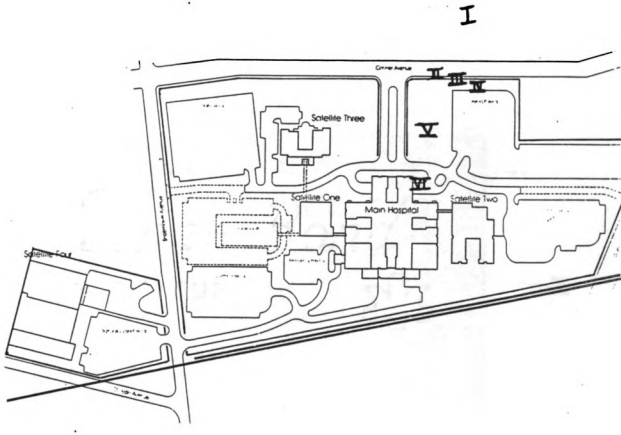
APPENDIX D

PHYSICAL SECURITY ZONES AND COUNTERMEASURES

SAMARITAN HEALTH CENTER
PHYSICAL SECURITY ARRANGEMENTS:
A GENERAL OUTLINE

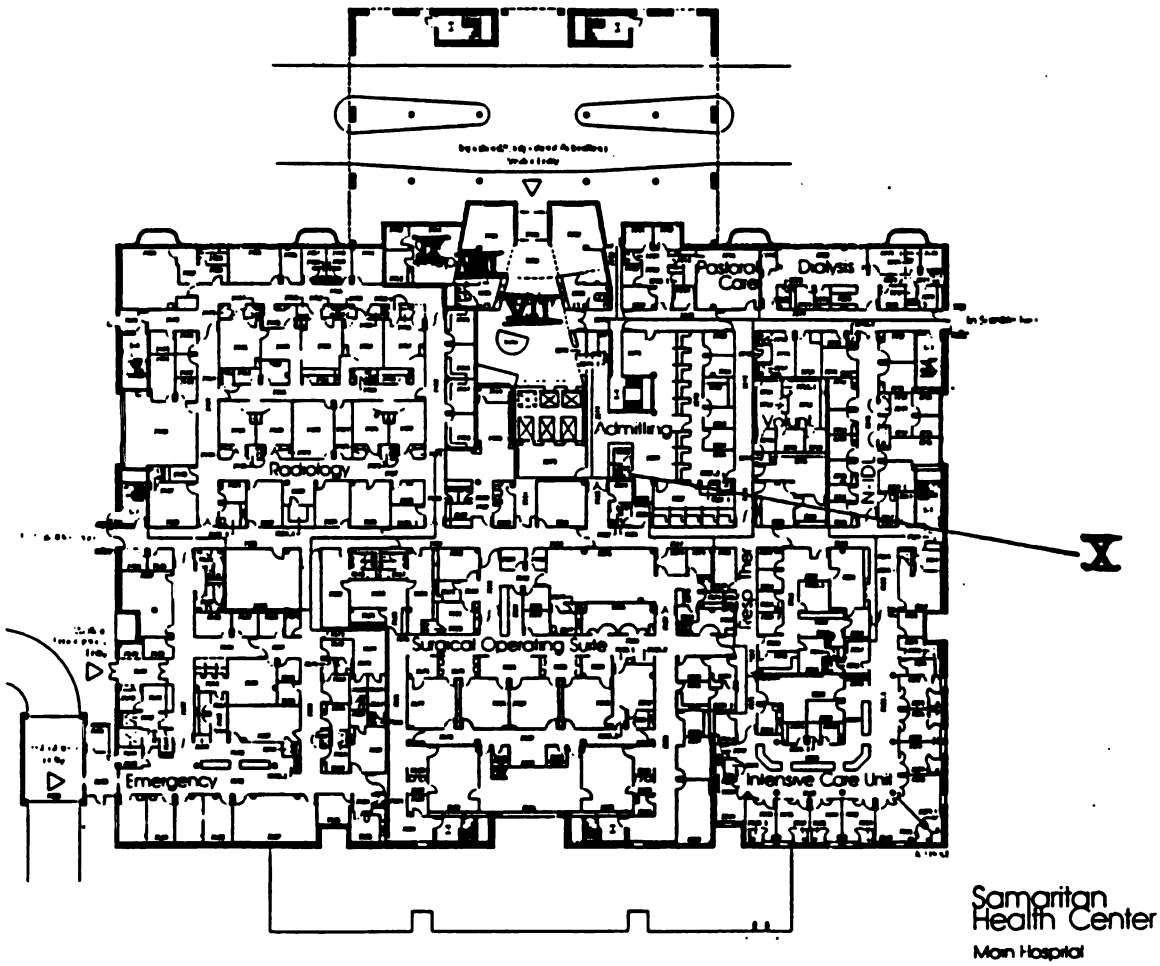
	Zones of Potential Vulnerability	Examples	Countermeasures Employed
I.	Neighborhood	The square mile of dwellings, businesses, streets and parks which surround the Health Center.	Lighting, Busstops, Traffic Lights, Streets as barriers.
II.	Adjacent Property	All grounds immediately encircling the boundary line, outward to a distance of 20 feet.	Lighting, Clear Zone.
III.	Boundary Line	The official limits or edge of Health Center property.	Lighting, Fencing, Restricted Entry/Exit, Clear Zone, C.C.T.V. Surveillance.
IV.	Adjacent Grounds	All grounds immediately encircled by the boundary line, inward to a distance of 20 feet.	Lighting, Clear Zone C.C.T.V. Surveillance, Patrols.
V.	General Grounds	Driveways, walkways, parking lots and lawns.	Lighting, Restricted Traffic Flow, Controlled Parking, Landscaping, Emergency Phones, C.C.T.V. Surveillance, Signage, Outdoor Posts, Patrols.
VI.	Building Exteriors	Employee/Visitor entrances fire exits, loading docks, windows, roof hatches.	Lighting, C.C.T.V. Surveillance, Emergency Phones, Intrusion Alarms, Fire Exit Alarms, Controlled Entry/Exit (Keys, Cards, Buzzer-Locks, Mag Locks), Signage, Patrols.
VII.	General Public Areas	Hallways, patient units, lobbies, cafeterias, rest rooms, waiting rooms, stairwells/elevators.	Lighting, C.C.T.V. Surveillance, Motion Detectors, Signage, Duress Alarms, Stair-well Lockdowns, Patrols, Indoor Posts.

	Zones of Potential Vulnerability	Examples	Countermeasures Employed
VIII.	Restricted Area Exteriors	Surgery, Mental Health Unit, Warehouse, Morgue, Laboratory, Pharmacy, Gift Shop, tunnel, Administration, Cashiers Office, Switchboard.	C.C.T.V. Surveillance, Intrusion Alarms, Controlled Entry/Exit (Keys, Cards, Buzzer-Locks, Mag Locks, Peep Holes), Bullet Resistant Glass, Signage, Patrols.
IX.	Restricted Area Interiors	Pharmacy and Laboratory Work Stations, Social Work and Mental Health Counselor's Offices, Gift Shop, Cashiers Office, Warehouse, tunnel.	C.C.T.V. Surveillance, Duress Alarms, Motion Detectors, Emergency Phones, Patrols.
X.	High Risk Points	Narcotics Vault, Security Directors Office, Med Carts, Master Key Cabinet, Cashiers Safe.	Intrusion Alarms, Duress Alarms, Controlled Access (Keys, Cards, Combination Locks).



Samaritan Health Center

Site Orientation


Pastoral Care
Dialysis
Admitting
Radiology
Surgical Operating Suite
Emergency
Intensive Care Unit
X
Samaritan Health Center
Main Hospital

APPENDIX E

PHILOSOPHY, MISSION, GOALS AND SCOPE OF SERVICES

Department of Protective Services
Samaritan Health Center

PHILOSOPHY

The Department of Protective Services at Samaritan Health Center is committed both in principle and practice to the overall Philosophy of the Sisters of Mercy Health Corporation.

In addition, the Department subscribes to the following tenets:

1) Quality healthcare services can only be provided within the context of a safe, secure and orderly environment.

2) All people within the healthcare environment are entitled certain basic rights, among them freedom from harm, reasonable fear of harm and property loss.

3) The value of human life is to be held paramount over all other concerns.

4) Human dignity must be preserved at all times, regardless of one's race, creed, religion, sex, nationality or socioeconomic status.

MISSION

The mission of the Department of Protective Services is to protect and serve the hospital, its patients, visitors, employees and medical staff. This shall be accomplished through the systemic and cost-effective integration of technology, personnel and prevention/control programs.

In carrying out this mission, the Department's primary areas of responsibility shall include: security, safety, fire protection, disaster preparedness, law enforcement and general assistance to those in need.

STRATEGIC GOALS

1) Prevention of security, safety, fire and disaster related incidents which may result in personal harm, property loss, legal liability or disruption of routine health care operations.

2) Minimization of the degree of harm, loss liability or disruption associated with those incidents which cannot be prevented.

3) Correction and/or elimination of the underlying problems which either cause or allow incidents to initially occur.

4) Provision of those miscellaneous services required for the general welfare and efficient operations.

SUPPORTIVE GOALS

5) The effective acquisition, development and maintenance of all departmental resources.

6) The effective utilization and management of all existing departmental resources.

7) Adherence to fiscal constraints on departmental resources in a cost-efficient manner.

8) A healthy organizational climate within the department which fosters positive working relationships and teamwork.

9) A positive image of the department within the health center and community which promotes confidence, trust, cooperation and favorable public relations.

10) Effective communication links within the department, the health center and the community.

SCOPE OF SERVICES

In keeping with its Philosophy, Mission and Goals the Department of Protective Services at Samaritan Health Center assumes primary operational responsibility for the following areas: security, safety, fire protection, emergency preparedness and general assistance. It operates 24 hours a day, seven days a week. Within this context the following activities are routinely undertaken by members of the department:

1) Continuous patrol of all health center buildings and grounds.

2) Enforcement of the health center's rules and regulations as well as the laws of the State of Michigan.

3) Investigation and documentation of security, safety and fire related incidents which occur on health center property.

4) Immediate response and management of security and safety related incidents as they occur.

5) Order maintenance on health center property, which shall include but not be limited to:
   - Access Control
   - Visitor Control
   - Parking and Traffic Control
   - Management of Civil disputes,
   - Patient restraint and Crisis intervention

6) Identification, reporting and correction of security, safety and fire related hazards.

7) Continuous monitoring of all security hardware systems such as:
   - cameras
   - intrusion alarms
   - holdup alarms

8) Immediate response and management of major emergency situations such as:
   - fire
   - explosion
   - bomb threat
   - civil disorder
   - power failure
   - telephone outage
   - radiation accident
   - tornado/severe thunderstorm
   - winter storm
   - other external disasters resulting in increased patient load

9) Periodic drills as they relate to the above mentioned emergencies.

10) Inservice training programs for health center personnel on security, safety and fire related topics.

11) Miscellaneous services to patients, visitors, and employees, such as:
- motorist assists
- employee escorts
- material transports
- directions and information
- patient valuables transfer
- lost-and-found

12) Package inspections.

13) Collection of visitor parking revenues and valet service.

14) Issuance and record keeping of the following:
- employee I.D. badges
- vehicle registrations
- keys

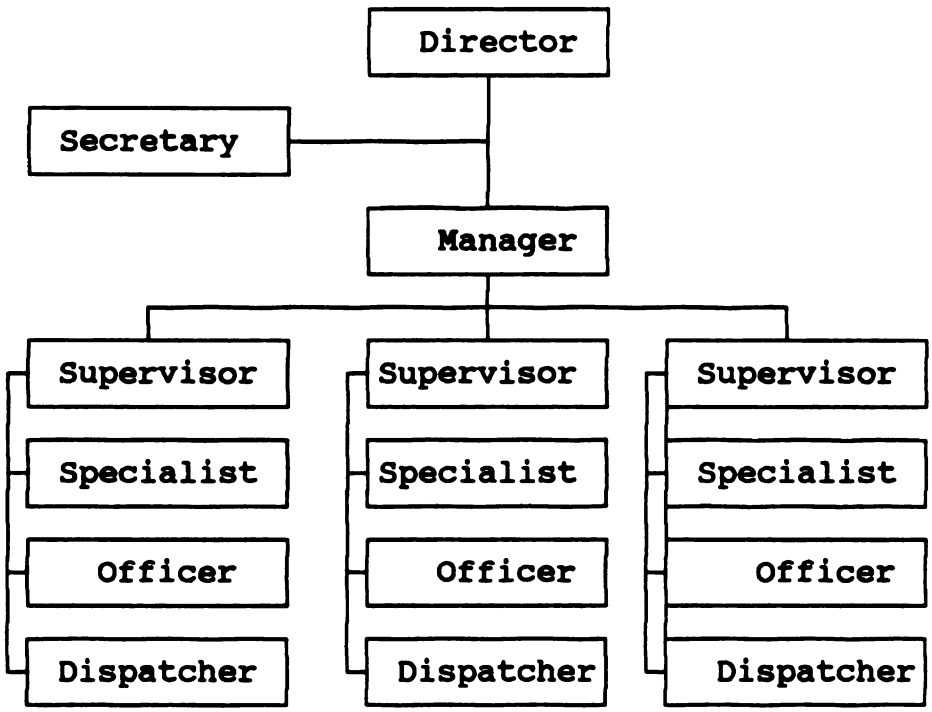
15) Periodic testing of all health center alarm systems, both security and fire.

16) Any other services required to maintain smooth health center operations.

APPENDIX F

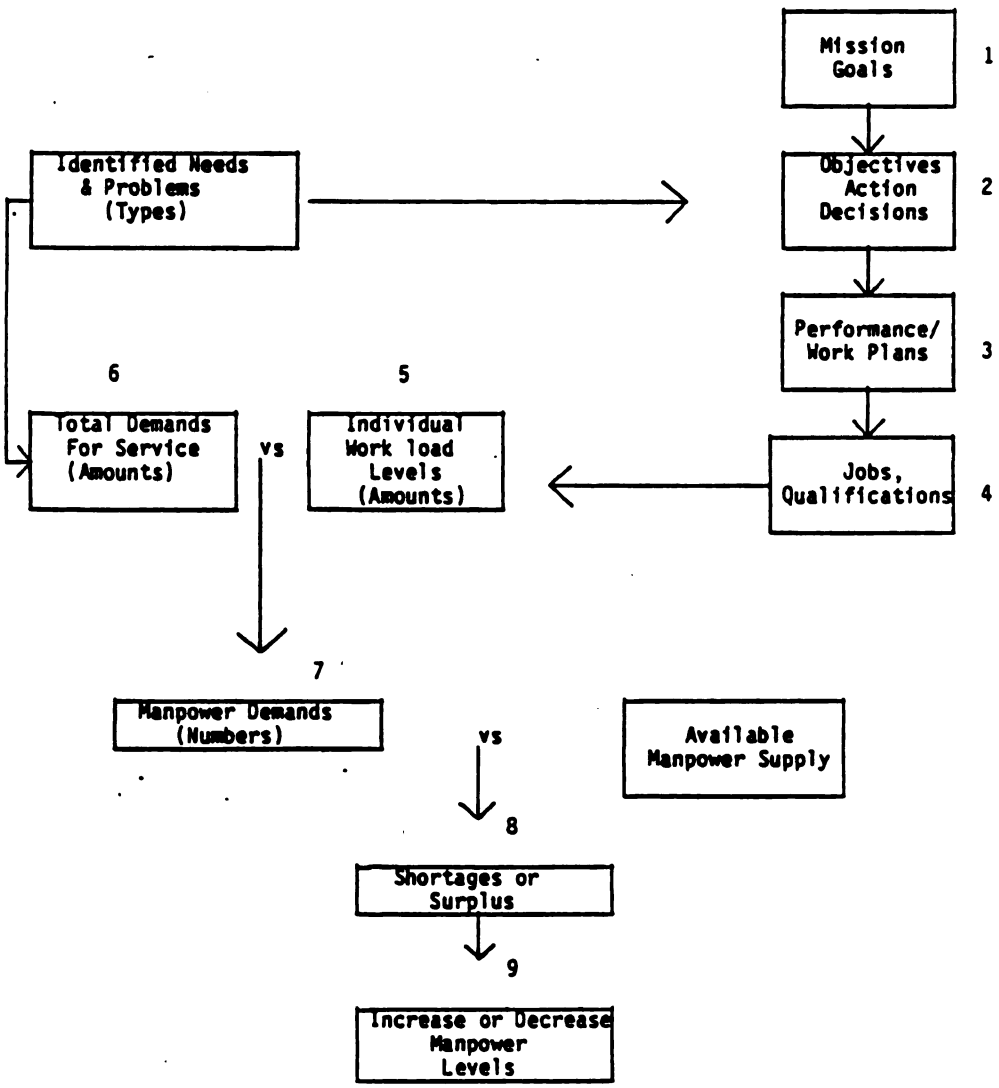
ORGANIZATIONAL CHART AND MANPOWER PLANNING GUIDES

DEPARTMENT OF PROTECTIVE SERVICES
ORGANIZATIONAL CHART



	No.
Director	1
Secretary	1
Manager	1
Supervisor	4
Specialist	21
Officer	9
Dispatcher	5
A.M. P.M. MID.	42

MANPOWER PLANNING WITH THE ACTION MODEL



MANPOWER PLANNING WORK SHEET

DEPARTMENT _____ TIME PERIOD LENGTH _____ JOB/POSITION _____

I. CALLS FOR SERVICE:

TYPE OF TASK/ACTIVITY/ RESPONSE	AVERAGE FREQUENCY OF OCCURRENCE	X	AVERAGE # OF PEOPLE NEEDED	X	AVERAGE TIME REQUIRED TO COMPLETE	+	AVERAGE TIME REQUIRED FOR REPORT WRITING	=	AVERAGE MAN-HOURS

TOTAL [ ]

II. ROUTINE ASSIGNMENTS: (i.e. required activities above and beyond Calls-for-Service)

PATROLS	AVERAGE # PER DAY	X	AVERAGE TIME REQUIRED	X	# OF DAYS	=	AVERAGE MAN-HOURS
POSTS							
OTHER							
					TOTAL		

III. FTE ADJUSTMENTS:

1) _____ (Calls for Service-Total Man-Hours) + _____ (Routine Assignments-Total Man-Hours) = _____ (Combined - Total Man-Hours Per Time Period)

2) _____ (Number of Time Periods in a Year) X _____ (Combined Total Man-Hours Per Time Period) = _____ (Total Man-Hours Per Year)

3) _____ (Total Man-Hours Per Year) ÷ _____ (Hours Worked Per FTE Per Year) = _____ (Total FTEs (Calls/Routine)

IV. REPLACEMENT NEEDS:

1) BREAKS/LUNCH _____ (Average Man-Hours Per Day Per FTE) X _____ (Days Worked Per FTE Per Year) X _____ (FTEs) = _____ (Man-Hours Per Year)

2) TRAINING _____ (Average Man-Hours Per FTE Per Year) X _____ (FTEs) = _____ (Man-Hours Per Year)

3) VACATION/HOLIDAYS _____ (Average Hours Per Day) X _____ (Days Per Year Per FTE) X _____ (FTEs) = _____ (Man-Hours Per Year)

4) SICK DAYS _____ (Average Hours Per Day) X _____ (Days Per Year Per FTE) X _____ (FTEs) = _____ (Man-Hours Per Year)

5) OTHER _____

_____ (Average Hours Per Day) X _____ (Days Per Year Per FTE) X _____ (FTEs) = _____ (Man-Hours Per Year)

V. FTE ADJUSTMENTS:

1) MAN-HOURS PER YEAR _____ (Breaks/ Lunch) + _____ (Training) + _____ (Vacation/ Holidays) + _____ (Sick Days) + _____ (Other) = _____ (Total Man-Hours Per Year)

2) _____ (Total Man-Hours Per Year) ÷ _____ (Hours Per FTE Per Year) = _____ (Total FTEs (Replacement))

VI. COMBINED TOTALS

_____ (Total FTEs (Calls/ Routine)) + _____ (Total FTEs (Replacements)) = _____ (Total FTEs)

APPENDIX G

DEPARTMENT MANUAL TABLE OF CONTENTS

TABLE OF CONTENTS

V. Routine Operations:
- Roll Call and Briefing
- Requesting and Providing Reliefs
- Leaving Health Center Property
- Radio Designations and Procedures
- Report Writing Procedures
- Post Duties and Procedures
- Patrol Duties and Procedures
- Zone Duties and Procedures
- Dispatch Duties and Procedures
- L.E.I.N. Computer Procedures
- Schedule of Routine Door Locks/Unlocks and Security Checks

VI. Special Procedures:
- "Stat" Calls
- Collecting Parking Revenue
- Motorist Assists
- Towing Procedures
- Police Contacts
- Accepting Subpoenas
- Key Control Procedures
- Opening Doors and Removing Property
- Property Transports
- Morgue Assists
- Lost and Found
- Visitor Control
- Maintaining Confidentiality
- Patient Search
- Visitor Search
- Staff Search
- Patient Restraint

VII. Legal Procedures:
- Arrests
- Lethal Force
- Non-lethal Force
- Search and Seizure
- Handling Evidence and Property
- Handling Prisoners
- Miranda Warnings
- Seeking Warrants
- Testifying in Court

VIII. Emergency Procedures:
- External Disaster
- Severe Weather
- Radiation Accident
- Hazardous Materials Accident
- Fire
- Bomb Threat/Explosion
- Gas Leak
- Power Outage
- Telephone Outage

Elevator Failure
Civil Disturbance

IX. Miscellaneous:
Maps
Phone Numbers
Forms

APPENDIX H

JOB DESCRIPTIONS

SAMARITAN HEALTH CENTER

JOB TITLE: Director-Protective Services
JOB FAMILY: Supervisory & Managerial

JOB CODE NO.: 4038
DEPARTMENT: Protective Services

EFFECTIVE: 07/01/86
REPORTS TO: Vice-President-Human Resource Services

F.L.S.A.: Exempt

GENERAL SUMMARY:

Under general direction maintains and develops SHC Protective Services in accordance with professional standards defined by accrediting services and SHC's policy and procedures. Plans, organizes, directs, controls and evaluates departmental services and establishes goals and objectives designed to realize the Philosophy and Mission of SHC.

TYPICAL DUTIES AND RESPONSIBILITIES

1. Directs and insures the provision of high quality protective services to all persons needing these services at SHC facilities.
2. Plans, directs and evaluates all departmental, technical and operational aspects.
3. Maintains Protective Services as defined by the appropriate licensing and accrediting agencies; Federal and State laws.
4. Responsible for departmental maintenance, repair and acquisition of supplies, equipment and material required in the performance of the department.
5. Maintains an effective working relationship with the SHC Management staff in matters pertaining to Protective Services.
6. Conducts investigations in connection with loss or theft of property, equipment and supplies and makes recommendation(s) to appropriate Health Center authorities.
7. Maintains close liaison with local, state and federal law enforcement agencies; and governmental Disaster Preparedness Agencies.
8. Orients and trains new staff as appropriate; and coordinates professional, technical, and clerical in-service, continuing education, and staff development programs for the department as required.
9. Develops, administers, and evaluates policies and procedures for the department in accordance with the Philosophy and mission of Samaritan Health Center, Quality Assurance Standards, J.C.A.H., M.D.P.H., and other agencies as required.

The primary purpose of this job description is to set a fair and equitable rate of pay for this classification. Only those key duties necessary for proper job evaluation and/or labor market analysis have been included. Other duties will be assigned by the supervisor.

10. Prepares, monitors, and evaluates departmental performance with respect to goals, and objectives, policies and procedures, budgets, professional and clerical staff requirements, reports, and other management functions as directed.

11. Performs administrative responsibilities to include maintaining records, writing reports and completing technical/statistical data.

QUALIFICATIONS

- Bachelor's degree in Law Enforcement, Criminal Justice or other related area or equivalent required.
- 5 - 7 years of professional experience required, hospital experience preferred.
- 3 - 5 years of managerial experience required, hospital experience preferred.
- Eligible for certification under the provisions of P.A. 330.
- Eligible to obtain a concealed weapons permit.

SAMARITAN HEALTH CENTER

TITLE:	Manager-Protective Services	JOB FAMILY:	Supervisory/Managerial
JOB CODE:	4094	DEPARTMENT:	Protective Services
EFFECTIVE DATE:	07/01/86	REPORTS TO:	Dir.-Protective Services
		F.L.S.A.:	Exempt

GENERAL SUMMARY:

Under general supervision assists in planning, administration and evaluation of the department, coordinates and/or conducts investigations, also manages routine operations and supervises subordinates.

TYPICAL DUTIES AND RESPONSIBILITIES

1. Coordinates and manages routine operations of a shift at the Health Center and P.C.I.'s, providing direct supervision of subordinate personnel and making job assignments.
2. Coordinates, manages and/or conducts investigations providing follow-up reporting and corrective action.
3. Reviews incident reports and payroll records to update and/or correct as necessary.
4. Prepares routine schedules ensuring adequate staffing is maintained at all times.
5. Assists in the preparation of statistical and narrative reports on security, safety, and fire related incidents, including the identification of trends and appropriate proposals for corrective or preventive action.
6. Oversees and reviews departmental equipment maintenance, needs and allocations making recommendations as necessary.
7. Assists in the development of departmental goals, objectives and related plans.
8. Assists in the development and implementation of departmental programs, policies and procedures and enforces them as necessary.
9. Assists in evaluation of department operations and effectiveness in providing protection.
10. Participates in the selection, training, supervision, evaluation, promotion, and discipline of subordinates.
11. Assists the Director in special projects or reports as requested.
12. Assumes responsibilities for the department in the Director's absence.
13. Enforces Health Center rules and regulations, department policies and procedures, and the laws of the State of Michigan.
14. Coordinates and directs a shift's response to emergency situations also evaluates and documents all actions taken.

The primary purpose of this job description is to set a fair and equitable rate of pay for this classification. Only those key duties necessary for proper job evaluation and/or labor market analysis have been included. Other duties will be assigned by the supervisor.

15. Oversees and/or reviews the conduct of subordinates with respect to arrests and physical interventions ensuring appropriate procedures are followed and documented.

16. Performs all of the duties of a subordinate as necessary.

QUALIFICATIONS

- Baccalaureate Degree in Criminal Justice, Security, Safety or other relevant discipline.
  AND
- 4 years of experience in the field. (Supervisory experience preferred).

  OR

- Master's Degree in Criminal Justice, Security, Safety or other relevant discipline.
  AND
- 2 years of experience in the field. (Supervisory experience preferred).

- Eligible for certification under the provisions of P.A. 330.

- Eligible to obtain a concealed weapon permit.

- Valid driver's license with a good driving record.

SAMARITAN HEALTH CENTER

JOB TITLE: Supervisor-Protective Services
JOB FAMILY: Supervisory/Managerial
JOB CODE NO.: 4092
DEPARTMENT: Protective Services
EFFECTIVE: 07/01/86
REPORTS TO: Director & Manager - Protective Services
F.L.S.A.: Exempt

GENERAL SUMMARY:

Under general supervision, directs and supervises protective services during the assigned shift.

TYPICAL DUTIES AND RESPONSIBILITIES:

1. Directs the routine activities of a shift at the Health Center or P.C.I.'s by assigning duties and supervising the performance of these duties.
2. Reviews, evaluates and recommends changes such as training, equipment, policy and procedure.
3. Supervises, conducts and/or assists in preliminary investigations of security, safety and fire related incidents. Takes corrective action as appropriate and forwards relevant information to Manager or Director.
4. Prepares, revises and adjusts routine schedules to accommodate manpower shortages and emergency situations.
5. Develops, reviews and corrects reports regarding all significant activities or incidents during the shift.
6. Participates in the selection of job applicants.
7. Evaluates the performance and behavior of subordinates informally, on an ongoing basis formally on a periodic basis, also provides appropriate motivational guidance and support.
8. Enforces departmental policies and procedures, as well as health center rules and regulations, disciplining subordinates as appropriate.
9. Enforces the laws of the State of Michigan.
10. Participates in the preservice training and orientation of new members, as well as inservice training and any other instructional programs.
11. Participates in the development and implementation of the departmental goals, objectives, plans, policies, procedures and programs.

The primary purpose of this job description is to set a fair and equitable rate of pay for this classification. Only those key duties necessary for proper job evaluation and/or labor market analysis have been included. Other duties will be assigned by the supervisor.

12. Oversees, directs, and/or reviews the conduct of subordinates with respects to arrests and physical confrontations, ensuring that appropriate procedures are followed and documented.

13. Coordinates and directs the response activities of the shift in all emergency situations, evaluates and documents those responses.

14. Performs all the duties of subordinates as necessary.

QUALIFICATIONS:

- Associates Degree in Criminal Justice, Security, Safety or other relevant discipline.
  AND
- 4 years of experience in the field.

  OR
- Baccalaureate Degree in Criminal Justice, Security, Safety or other relevant discipline.
  AND
- 2 years of experience in the field.

  OR
- Masters Degree in Criminal Justice, Security, Safety or other relevant discipline.

  AND
- 1 Year of experience in the field.
- Eligible for certification under the provisions of P.A. 330.
- Eligible to obtain a concealed weapon permit.
- Valid drivers license with good driving record.

SAMARITAN HEALTH CENTER

JOB TITLE: Protective Services Specialist JOB FAMILY: Office & Administrative

JOB CODE NO.: 1132 DEPARTMENT: Protective Services

EFFECTIVE DATE: 07/01/86 REPORTS TO: Manager

F.L.S.A.: Non-Exempt

GENERAL SUMMARY:

Under direct supervision protects and serves the Health Center, its patients, visitors and employees. Ensures a safe, secure and orderly environment. Patrols the Health Center's buildings and grounds; observing, reporting, responding to and correcting hazardous situations.

TYPICAL DUTIES AND RESPONSIBILITIES:

1. Protects patients, visitors and employees from harm and reasonable fear of harm.
2. Maintains an acceptable level of order, control and safety on the premises.
3. Protects personal and Health Center property from theft, misuse and vandalism.
4. Conveys an image of professionalism, behaving in a way that is conducive to good Health Center and community relations.
5. Conducts fire, safety and security inspections, reporting and correcting hazards as necessary.
6. Provides zone and patrol coverage throughout the Health Center and P.C.I.'s responding to security and safety related incidents as needed.
7. Responds to major emergency situations at the Health Center and P.C.I.'s i.e. fights, fires, conducts bomb threat searches and takes any other action necessary to protect lives and property.
8. Develops accurate and detailed reports on all significant security, safety, and fire related activities and incidents, conducting preliminary investigations as necessary.
9. Serves as shift "leader" whenever assigned. Coordinates routine operations, directs the activities of other personnel and assumes functional charge of the shift as assigned.
10. Staffs the operations center, providing alarm and camera monitoring, radio dispatching and switchboard relief for telephone operators as assigned.
11. Enforces Health Center rules and regulations, as well as the laws of the State of Michigan.
12. Conducts visitor, patient and/or employee searches as directed.

The primary purpose of this job description is to set a fair and equitable rate of pay for this classification. Only those key duties necessary for proper job evaluation and/or labor market analysis have been included. Other duties will be assigned by the supervisor.

13. Controls the flow of traffic and visitors throughout the Health Center.

14. Performs all the duties of a Protective Services Officer as necessary.

15. Provides miscellaneous services to patients, visitors and employees; such as information, directions, assists, and escorts.

QUALIFICATIONS:

- High School Diploma or G.E.D. equivalent.
  AND
- 3 years of experience in security, safety or related field.

  OR

- Any combination of 3 years or experience and college education in Criminal Justice, Security, Safety or related field.

  OR

- Baccalaureate Degree in Criminal Justice, Security, Safety or other relevant discipline.

- Eligible for certification under the provisions of P.A. 330.

- Valid driver's license with good driving record.

- Eligible to obtain a concealed weapons permit.

SAMARITAN HEALTH CENTER

JOB TITLE: Protective Services Officer
JOB CODE NO.: 1131
EFFECTIVE DATE: 07/01/86
JOB FAMILY: Office & Administrative
DEPARTMENT: Protective Services
REPORTS TO: Mgr.-Protective Services
F.L.S.A.: Non-Exempt

GENERAL SUMMARY:

Under direct supervision protects and serves the Health Center, its patients, visitors and employees. Maintains post assignments at the P.C.I.'s and the Health Center's major parking lots; observing, reporting, responding to and correcting hazardous situations.

TYPICAL DUTIES AND RESPONSIBILITIES:

1. Protects patients, visitors, and employees from harm and reasonable fear of harm.
2. Maintains an acceptable level of order, control and safety on the premises.
3. Protects personal and Health Center property from theft, misuse and vandalism.
4. Conveys an image of professionalism, behaving in a way that is conducive to good Health Center and community relations.
5. Maintains an acceptable level of order, control and safety on the premises.
6. Protects personal and Health Center property from theft, misuse and vandalism.
7. Conveys an image of professionalism, behaving in a way that is conducive to good Health Center and community relations.
8. Identifies, reports and corrects hazards as necessary.
9. Maintains post assignments at the P.C.I.'s and the Health Center's major parking lots, responds to security and safety related incidents as needed.
10. Controls the flow of traffic at the visitor and administrative complex parking lots and provides surveillance of those areas. Collects and processes parking revenue at visitor lot.
11. Responds to major emergency situations, i.e. fights, fires, conducts bomb threat searches and takes any other action necessary to protect lives and property.
12. Develops accurate and detailed reports on all significant security, safety and fire related activities and incidents.
13. Enforces Health Center rules and regulations and assists Protective Services Specialists and Managers, upon request, in the enforcement of the laws of the State of Michigan.

The primary purpose of this job description is to set a fair and equitable rate of pay for this classification. Only those key duties necessary for proper job evaluation and/or labor market analysis have been included. Other duties will be assigned by the supervisor.

14. Provides miscellaneous services to patients, visitors, and employees; such as information, directions, assists, and escorts.

QUALIFICATIONS:

- High School Diploma or G.E.D. equivalent.
- 1 - 2 years of Security, Safety or related experience/education preferred.
- Eligible for certification under the provisions of P.A. 330.
- Valid driver's license with good driving record required.

SAMARITAN HEALTH CENTER

JOB TITLE: Protective Services Dispatcher
JOB FAMILY: Office & Administrative
JOB CODE NO.: 1135
DEPARTMENT: Protective Services
EFFECTIVE: 07/01/86
REPORTS TO: Supervisor-Protective Services or Shift Leader
F.L.S.A.: Non-Exempt

GENERAL SUMMARY:

Under direct supervision, staffs the operations center, maintaining and coordinating radio communications, monitoring alarm and surveillance equipment, answering telephones and performing routine clerical functions.

TYPICAL DUTIES AND RESPONSIBILITIES:

1. Coordinates all radio communications and dispatches personnel to requests for service, both routine and emergency.
2. Monitors closed circuit television cameras and operates the video tape recorder.
3. Monitors all security and fire alarm systems.
4. Operates the access control computer.
5. Answers the telephone and provides general information.
6. Maintains communication links with local police and fire departments as necessary.
7. Provides relief on hospital switchboard in the absence of switchboard operators.
8. Performs routine clerical and typing functions as required.
9. Maintains accurate and up-to-date records such as. daily activity log, property/evidence book, complaint/incident book, arrest book, alarm tests, and emergency preparedness drill documentation.
10. Provides miscellaneous services to patients, visitors and employees as requested such as giving location directions and transporting patients.

QUALIFICATIONS:

- High School diploma or equivalent.
- Eligible for certification under the provisions of P.A. 330.
- Accurate typing skills.
- Previous security and/or dispatching experience preferred.

The primary purpose of this job description is to set a fair and equitable rate of pay for this classification. Only those key duties necessary for proper job evaluation and/or labor market analysis have been included. Other duties will be assigned by the supervisor.

SAMARITAN HEALTH CENTER

JOB TITLE: Secretary

JOB CODE NO.: 1082

EFFECTIVE: 04/29/88

JOB FAMILY: Office and Administrative

DEPARTMENT: Intra-Health Center

REPORTS TO: Varies

F.L.S.A.: Non-Exempt

GENERAL SUMMARY:

Under limited supervision performs a variety of routine and complex information systems, clerical and secretarial duties within a department. Individuals assigned to this classification have work assignments which are characterized by (a) thorough knowledge and understanding of departmental policies, procedures and practices, (b) advanced skills in information systems, typing, general clerical and secretarial duties, (c) providing some level of direct support to the department director or a group of supervisors and (d) may relieve the supervisor of some administrative tasks which are routine in nature.

TYPICAL DUTIES AND RESPONSIBILITIES:

1. Completes a wide range of typing assignments which include letters, lists, tables, charts, memoranda, records, forms and so forth using a personal computer, word processor, typewriter, calculator and/or transcription equipment to input and update information.

2. Creates department personal computer systems, using soft-ware packages to assimilate forms/reports and inputs departmental data (on diskettes or hard disk) as required, depending on department assignment.

3. Proofreads and edits draft and final copy materials for appropriate and consistent format, accuracy of financial figures or other data and correct spelling, punctuation and grammar.

4. Arranges and plans meetings and conferences, schedules interviews and appointments, completes travel arrangements and maintains personal calendars.

5. May assist in the preparation of Administrative reports, statements, rosters and so forth. Performs routine data or information gathering; computes calculations and drafts routine, special reports or summaries for review by supervisor.

6. Receives and screens visitors and telephone calls and either notifies superior or other staff members or records and relays messages. Responds to general inquiries concerning the activities and operation of the department.

7. Routinely engages in contacts outside of the hospital in order to relay information concerning departmental services, answering inquiries, making arrangements and so forth.

The primary purpose of this job description is to set a fair and equitable rate of pay for this classification. Only those key duties necessary for proper job evaluation and/or labor market analysis have been included. Other duties will be assigned by the supervisor.

8. Gathers data from departmental records and prepares, completes and/or processes reports, records, billings and so forth that require an understanding of departmental or unit policies and procedures.

9. Establishes and maintains recordkeeping and filing systems, classifies, sorts and files correspondence, articles, records and other documents.

10. May assist in the preparation of procedure manuals and other departmental documentation as assigned.

11. Requisitions regularly used office supplies and assists in the maintenance of adequate supply levels.

12. May coordinate department clerical and/or volunteer services.

13. Opens, sorts and distributes departmental mail.

QUALIFICATIONS:

- High School or equivalent required.
- 1 - 2 years of related experience required.
- Excellent typing skills required.

APPENDIX I

TRAINING CURRICULUM OUTLINE

SAMARITAN HEALTH CENTER

DEPARTMENT OF PROTECTIVE SERVICES

CERTIFICATION TRAINING CURRICULUM

SECTION	TOPIC	HOURS
Administrative Section:	Public Act 330 & The State Police	2
	Department Procedures	4
		6
Legal Section:	Admissions & Confessions	2
	Constitutional Law	2
	Court Functions	4
	Juvenile Law	3
	Laws of Arrest	7
	Search and Seizure	5
	Laws of Evidence	5
	Criminal Law	10
		38
Investigative Section:	Investigations	5
	Narcotics & Drugs	2
		7
General Section:	Patrol Techniques	10
	Firearms	46
	BCLS/Bleeding/Shock	10
	Radio Communications	2
	Report Preparation	6
	Traffic Direction & Control	1
	Crowd Behavior	2
	Defensive Tactics	8
	Lamb Baton	6
	Handgun Retention	2
	Search/Arrest Techniques	2
		95

SECTION	TOPIC	HOURS
Special Section:	Courtesy & Ethics	2
	Human Relations	2
	Handling Disturbed Persons	8
	Stress Management	1
	Fire Protection	10
	Bombs	4
	Emergency Preparedness	2
	Safety	4
	Lifting & Transporting	2
	Risk Management	1
	Crime Prevention	5
		42
Health Care Perspective:	Hospital Orientation	3
	Hospital Tour	3
	Hospital Organization	1
	Special Problems in Healthcare	1
	Department Organization & Functions	1
	Hospital Services & Security	3
		12
Testing:	Firearms	2
	Legal Section	2
	Misc. Topics	4
		8

200 Hours of Total Instruction
8 Hours of Testing
24 hours of OJT.
8 hours of General Orientation

NOTE: In addition to written tests on all topics covered, the following topics also have "hands-on" proficiency tests included during the training sessions:

Firearms
Defensive Tactics
Lamb Baton
Arrest/Search Techniques
Handling Disturbed Persons
Lifting & Transporting
Handgun Retention
B.C.L.S.
Fire Protection
Patrol Techniques

APPENDIX J

HOSPITAL POLICY AND PROCEDURE STATEMENT

HEALTH/SAFETY 09/01/86 9.05

1 of 4

PROTECTIVE SERVICES

V. P., Human Resources

Applies: ALL EMPLOYEES, VISITORS, PATIENTS AND MEDICAL STAFF

I. POLICY

It is the policy of Samaritan Health Center to provide for the security and safety of all persons on the property. This shall be accomplished through the cost-effective integration of physical security/safety controls, competent personnel and comprehensive loss prevention programs.

II. REGULATIONS AND DEFINITIONS

A. Personnel

The Health Center shall maintain at all times a sufficiently staffed Department of Protective Services, within available resources.

B. Responsibilities

1. The department shall be given primary responsibility for maintaining a safe, secure and orderly environment.

2. The department shall also be responsible to enforce the rules and regulations of the Health Center as well as the laws of the State of Michigan.

C. Training

Relevant training and professional development opportunities shall be provided to all Department of Protective Services personnel on a regular basis, within available resources.

D. Programs

1. The department shall plan, develop and implement specific programs relating to security, safety, fire protection and emergency preparedness. This shall be accomplished both independently and as appropriate in conjunction with other Health Center departments and personnel.

2. All programs shall be developed to satisfy both current problems and projected needs. These problems and needs shall be assessed and reviewed on an ongoing basis.

E. Evaluation

The effectiveness of both individual programs and overall department operations shall be evaluated at least annually, with appropriate changes being made as deemed necessary.

III. PROCEDURE

RESPONSIBILITY	ACTION
Department of Protective Services	1. Continuously patrol all Health Center buildings and grounds.
	2. Enforce the Health Center's rules and regulations as well as the laws of the State of Michigan.
	3. Investigate and document security, safety and fire related incidents which occur on Health Center property.
	4. Respond to and manage security and safety related incidents as they occur.
	5. Maintain order on Health Center property, including but not limited to the following areas: Access Control Visitor Control Parking and Traffic Control Management of Civil disputes Patient restraint and Crisis intervention
	6. Identify, report and correct security, safety and fire related hazards.
	7. Monitor all security hardware systems, such as: cameras intrusion alarms holdup alarms

RESPONSIBILITY	ACTION
	8. Respond to and manage major emergency situations, such as: fire explosion bomb threat civil disorder power failure telephone outage radiation accident tornado/severe thunderstorm winter storm other external disasters resulting in increased patient load
	9. Conduct periodic drills as they relate to the above mentioned emergencies.
	10. Provide inservice training programs for Health Center personnel on security, safety and fire related topics.
	11. Provide miscellaneous services to patients, visitors, and employees, such as: motorist assists employee escorts directions and information lost and found
	12. Conduct inspections of personal and Health Center property leaving the premises.
	13. Issue control and keeps records of the following: employee I.D. badges vehicle registrations keys

RESPONSIBILITY	ACTION
	14. Conduct periodic testing of all Health Center Alarm systems, both security and fire.
	15. Provide any other services required to maintain smooth Health Center operations.
Administration	1. Provide the authority, support and resources (within availability) necessary for the Department of Protective Services to effectively carry out its role.
All Employees	1. Observe sound security, safety and fire prevention practices.
	2. Obey the Health Center's rules and regulations pertaining to security and safety.
	3. Cooperate with and assist Department of Protective Services personnel whenever requested to do so.
	4. Report all security, safety and fire hazards immediately.
	5. Actively participate in all emergency preparedness drills and related inservice training programs.

APPENDIX K

ZERO BASED BUDGETING GUIDES

Z.B.B. DECISION PACKAGE RANKING SHEET

RANK	PACKAGE NAME	FY__ BUDGET	FY__ REQUEST	% Δ	CUMULATIVE	
					FY REQUEST	% Δ

ZBB DECISION PACKAGE

PACKAGE NAME	DEPARTMENT	ACCOUNTABLE INDIVIDUAL	FISCAL YEAR	RANK

I. PURPOSE/RELATED OBJECTIVE(S)	
PRIORITY OF OBJECTIVE(S)	
II. DESCRIPTION/EXPLANATION OF THE ACTION DECISION/ACTIVITY (INCLUDING SUMMARY OF RELATED TASKS, DUTIES, ETC. AS APPROPRIATE)	
III. SPECIFIC RESULTS/ACHIEVEMENTS EXPECTED (INCLUDING APPROPRIATE QUANTITATIVE MEASURES)	

IV. CONSEQUENCES OF NOT APPROVING

V. REQUIRED RESOURCES	PERSONNEL	COSTS			FRINGE COSTS			SUPPLIES	COSTS			EQUIPMENT	COSTS			OTHER	COSTS		
		FY_	FY_	%Δ	FY_	FY_	%Δ		FY_	FY_	%Δ		FY_	FY_	%Δ		FY_	FY_	%Δ
(Include types and amounts as appropriate)																			
SUBTOTALS								X				X				X			

PACKAGE TOTAL		
FY	FY	% Δ

Reader's Note: This page has been condensed for illustrative purposes. In reality the columns should be widened and two pages would be needed.

VI. POSSIBLE ALTERNATIVES FOR THIS ACTION DECISION/ACTIVITY	i.e. LESSER DEGREES/LEVELS AT WHICH THIS ACTION DECISION/ACTIVITY COULD BE CARRIED OUT. (Other than at the preferred degree/level)	SUMMARY OF REQUIRED RESOURCES AND COSTS	SUMMARY OF RELATIVE BENEFITS AND DISADVANTAGES
1)			
2)			
VII. POSSIBLE ALTERNATIVE ACTION DECISIONS/ ACTIVITIES	**i.e. DIFFERENT ACTION DECISIONS/ACTIVITIES FOR ACHIEVING THE SAME PURPOSE/RELATED OBJECTIVE(S) (Other than the preferred action decision/activity)**	**SUMMARY OF REQUIRED RESOURCES AND COSTS**	**SUMMARY OF RELATIVE BENEFITS AND DISADVANTAGES**
1)			
2)			

APPENDIX L

REORGANIZATION PROPOSAL TABLE OF CONTENTS

TABLE OF CONTENTS

Below is a listing of the major components of the proposed reorganization plan. Each one will be presented in greater detail on the pages indicated:

APPENDIX M

MAJOR PHYSICAL SECURITY SYSTEM COMPONENTS

SAMARITAN HEALTH CENTER
SECURITY & SAFETY HARDWARE SYSTEM:
A SUMMARY OF MAJOR COMPONENTS

Computerized Fire Protection Sub-System - Simplex Fire Protection Computer
- 2 C.R.T. Consoles & Printer
- Magnetic Locks
- Automatic Smoke/Fire Doors
- Manual Pull Boxes
- Sprinkling System
- CO_2 Fire Suppression System
- Halon System
- Fire Extinguishers/Hoses
- Smoke Detectors
- Waterflow Detectors
- Heat Detectors
- Fire Shutters
- Stand Pipes & Hydrants & P.I.V.'s
- Audible Alarms
- P.A. System
- Emergency Hotline Number
- Individualized Zoning of Alarm Signals and Safety Releases
- Redundancy with Security Computer

Computerized Security Sub-System - Digital Access Control Computer
- 3 C.R.T. Consoles & 2 Printers
- Micro-Computer Backup with Fail Soft Capability
- 10 M byte Memory with 2 Floppy Disks
- Complete Report, Time/Attendance, Dr's Registry Capabilities
- U.P.S.
- ID/Access Cards with Wiegand Technology
- "Slide through" Card Readers
- Duress Alarms
- Intrusion Alarms
- Intercom/Buzzer Locks
- Motion Detectors
- Bullet Resistant "Lexguard" Glass & Pass Through Drawers
- Magnetic Locks with Local Alarms
- Detex Fire Exit Alarms
- Combination Locks
- Emergency Phones with Direct Dial
- Outdoor Cameras (P/T & Zoom, fixed)
- Indoor Cameras (fixed)
- C.C.T.V. Monitors with Sequential Switching and Controls
- V.T.R. and display monitor

Communications Sub-System	- Kenwood Radio Communications System • Repeater • Base Station • Mobile Radio's • Portable Radio's • Rapid Chargers
Key Control Sub-System	- Schlage "High Security " keys & locks. • Each Department mastered separately. • Each Building grand-mastered separately. • Full accountability over distribution, record-keeping, storage and retrieval of keys. • Internal control over duplication of blanks and repair/replacement of locks. • Coding system for labeling of keys.

BIBLIOGRAPHY

BIBLIOGRAPHY

Books

Anderson, Sconvia, B. The Profession and Practice of Program Evaluation. San Francisco: Jossey-Bass, 1978.

Appley, Lawrence A. Manpower Planning: A Professional Management System. New York: AMACOM, 1981.

Astor, Saul D. Loss Prevention: Controls and Concepts. Los Angeles, CA: Security World Publishing Co., 1978.

Bartholomew, David J. and Andrew F. Forbes. Statistical Techniques for Manpower Planning. New York: Wiley, 1979.

Bates, Donald L. Strategy and Policy: Analysis Formulation and Implementation. Dubuque, Iowa: W. C. Brown Co., 1980.

Bennis, Warren. Changing Organizations. New York: McGraw-Hill, 1966.

Berger, David L. Industrial Security. Los Angeles, CA: Security World Publishing Co., 1979.

Buckley, Walter. Sociology and Modern Systems Theory. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1967.

Burack, Elmer H. Human Resource Planning: A Pragmatic Approach to Manpower Staffing and Development. Lake Forest, IL: Brace-Park Press, 1980.

Burnstein, Harvey. Hospital Security Management. New York: Praeger Publisher, 1977.

Burnstein, Harvey. Industrial Security Management. New York: Praeger Publishers, 1977.

Carroll, Stephen J. Management by Objectives: Applications and Research. New York: Macmillan, 1973.

Craig, Dorothy P. Hip Pocket Guide to Planning and Evaluation. Austin, TX: Learning Concepts, Inc., 1978.

Cole, Richard B. The Application of Security Systems and Hardware. Springfield, IL: Charles C. Thomas, 1970.

Cole, Richard B. Protection Management and Crime Prevention. Cincinnati, Ohio: W. H. Anderson Company, 1974.

Colling, Russell. Hospital Security. Los Angeles: Security World Publishing Co., Inc., 1976.

Colling, Russell L. Hospital Security. Second Edition. Boston: Butterworths Publishers, 1982.

Cunningham, William C. and Todd H. Taylor. Crime and Protection in America: A Study of Private Security and Law Enforcement Resources and Relationships. McLean, VA: Hallcrest Systems, Inc., 1985.

Dillan, Roy D. Zero-Base Budgeting for Healthcare Institutions. Germantown, MD: Aspen Systems Corp., 1979.

Epstein, Irwin. Research Techniques for Program Planning, Monitoring & Evaluation. N.Y.: Columbia University Press, 1977.

Fennelly, Lawrence J. Handbook of Loss Prevention and Crime Prevention. Boston: Butterworth Publishers, 1982.

Fisher, James A. Security for Business and Industry. Englewood Cliffs, NJ: Prentice-Hall, 1979.

Gallati, Robert R. J. Introduction to Private Security. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1983.

Green, Gion and Raymond C. Farber. Introduction to Security. Los Angeles, CA: Security World Publishing Co., Inc., 1975.

Green, Gion. Introduciton to Security. 3rd Ed. Woburn, MA: Butterworth Publishers, Inc., 1981.

Grinold, Richard C. Manpower Planning Models. New York: North-Holland Pub. Co., 1977.

Healy, Richard. Design for Security. New York: John Wiley & Sons, 1968.

Healy, Richard J. and Timothy J. Walsh. Industrial Security Management: A Cost Effective Approach. New York: American Management Association, Inc., 1971.

Healy, Richard J. and Timothy J. Walsh. Principles of Security Management. Long Beach, CA: Professional Publications, 1981.

Hemphill, Charles F., Jr. Management's Role in Loss Prevention. New York: AMACON, 1976.

Hemphill, Charles F., Jr. Modern Security Methods. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1979.

Hemphill, Charles F., Jr. Security for Business and Industry. Homewood, ILL: Dow-Jones-Irwin Inc., 1979.

Humble, John William (Ed.) Management by Objectives in Action. New York: McGraw-Hill, 1970.

Jeffrey, C. Ray. Crime Prevention Through Environment Design. Beverly Hills, CA: Sage Publications, 1971.

Kakalik, James S. and Sorrel Wildhorn. Private Police in the United States: Findings and Recommendations, Vol. 1. Santa Monica: The Rand Corporation, 1972.

Kakalik, James S. and Sorrel Wildhorn. The Private Police-Security and Danger. New York: Crane Russak, 1977.

Kingsbury, Arthur A. Introduction to Security and Crime Prevention Surveys. Springfield, ILL: Charles C. Thomas Publishing Co., 1973.

Leichenstein, Michael. Designing for Security. New York: Rand Institute, 1971.

Mandlebaum, Albert J. Fundamentals of Protective Systems. Springfield, ILL: Charles C. Thomas, 1973.

Morneau, R. H., Jr., and G. E. Morneau. Security Administration: A Quantitative Handbook. Woburn, MA: Butterworth Publishers, Inc., 1982.

Morse, George P. Protecting the Health Care Facility: A System of Loss Prevention. Baltimore, MD: The Williams and Wilkins Company, 1974.

Morse, George P. and Robert F. Morse. Protecting the Health Care Facility. Baltimore: The Williams and Wilkins Co., 1974.

Newman, Oscar. Defensible Space. New York: Macmillan Company, 1972.

O'Block, Robert L. Security and Crime Prevention. St. Louis, MO: C.V. Mosby Company, 1979.

Odiorne, George S. Management by Objectives: A System of Managerial Leadership. New York: Pittman Pub. Corp., 1965.

Paine, David. Basic Principles of Industrial Security. Madison, WI: Oak Security Publications, 1972.

Pascal, Michael A. Hospital Security and Safety. Germantown, MD: Aspen, Systems Corp., 1977.

Patten, Thomas H., Jr. Manpower Planning and the Development of Human Resources. New York: John Wiley & Sons, 1971.

Post, Richard S. Determining Security Needs. Madison, WI: Oak Security Publications, 1973.

Post, Richard S. and Arthur A. Kingsbury. Determining Security Needs. Madison, WI: Oak Security Publications, 1973.

Post, Richard S. and Arthur A. Kingsbury. Security Administration. 3rd Ed. Springfield, ILL: Charles C. Thomas, 1977.

Post, Richard S. and David A. Schachtsiek. How to Develop an Effective Company Security Program. Chicago: Dartnell Corporation, 1977.

Ricks, Truett A., et al. Principles of Security, An Introduction. Cincinnati, OH: Anderson Publishing Company, 1981.

Ross Laboratories. Hospital Security Manual. Columbus, OH 1975.

Schultz, Donald O. Principals of Physical Security. Houston, TX: Gulf Publishing Co., 1978.

Smith, Nick L. New Techniques for Evaluation. Beverly Hills: Sage, 1981.

Smith, Robert A. Hospital Security Management. Lansing: Michigan Hospital Association, 1983.

Seenewald, Charles. Effective Security Management. Woburn, MA: Butterworth Publications, Inc., 1978.

Sower, Christopher. Community Involvement. Glencoe, IL: The Free Press, 1957.

Strauss, Sheryl, Ed. Security Problems in a Modern Society. Boston, MA: Butterworth Publications, Inc., 1980.

Strobl, Walter M. Crime Prevention Through Physical Security. Knoxville, Tennessee: Training Consultants, Inc., 1978.

Strobl, Walter M. Handbook for Hospital Security Personnel. Knoxville, Tennessee: Training Consultants, Inc., 1977.

Trojanowicz, Robert C. Juvenile Delinquency: Concepts and Control. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1973.

Ursic, Henry S. and Leroy E. Pagano. Security Management Systems. Springfield, ILL: Charles C. Thomas Publishing Co., 1972.

Van de Vein, Andrew H. Measuring and Assessing Organizations. N.Y.: Wiley, 1980.

Varney, Glenn H. Management by Objectives. (2nd Ed.) Chicago: Dartnell Corp., 1979.

Walker, James W. Human Resource Planning. NY: McGraw-Hill, 1980.

Walsh, Timothy and Richard Healy. Protection of Assets. Santa Monica, CA: Merritt Company, 1976.

Warren, Roland L. Social Change and Human Purpose: Toward Understanding and Action. Chicago: Rand McNally Publishing Company, 1971.

Woodruff, Ronald S. Industrial Security Techniques. Columbus, OH: Charles E. Merrill Publishing Co., 1974.

Young, Ken M. The Basic Steps of Planning. Charlottesville, VA: Community Collaborations, 1978.

Zaltman, Gerald and Robert Duncan. Strategies for Planned Change. New York: John Wiley & Sons, 1977.

Articles

_____ "Action Plan for Hospital's Total Security." Security World, Vol. 16, No. 8, August 1979.

Bhada, Y. K. and G. Mimmier. "Integrate Z.B.B. into your M.B.O. Framework." Financial Executive, Vol. 48, No. 42, June 1980.

Brodie, James L. "Health Care Facilities." Handbook of Building Security Planning and Design. Peter S. Hopf, Ed. New York: McGraw-Hill, 1979.

Cartwright, Timothy. "Problems, Solutions, and Strategies: A Contribution to the Theory and Practice of Planning." Journal of the American Institute of Planners, May 1973.

Cole, Richard B. "Designing for Security." Progressive Architecture, November, 1970, p. 84 - 89.

Frisbie, Douglas. "Crime Analysis in Crime Prevention Planning." Handbook of Loss Prevention and Crime Prevention, edited by Lawrence J. Fennelly. Boston: Butterworths Publishers, 1982.

Girard, Charles M. "Planning, Management and Evaluation: Important Tools to the Crime Prevention and Security Officer." Handbook of Loss Prevention and Crime Prevention, edited by Lawrence J. Fennelly. (Boston: Butterworths Publishers, 1982.

Great Lakes Chapter of the International Association for Hospital Security. "Hospital Security." Michigan Hospitals, October 1981, (entire issue).

Howlett, Fred and Hunter Hurst. "A Systems Approach to Comprehensive Criminal Justice Planning." Crime and Delinquency, Vol. 18, No. 4, October 1971.

Jaspan, Norman and Walter Nagel. "Theft in the Health Care Industry." Topics in Health Care Financing, Aspen Publication, Winter 1978.

Smith, Robert A. "A Systems Approach to Loss Prevention in Hospitals." Journal of Security Administration, Vol. 4, No. 2, 1981.

Sower, Christopher. "An Experimental Sociology of Institutional Renewal." Rural Sociology, Vol. 41, No. 1, Spring 1976, p. 13.

Swartz, B. N. "Bringing Zero-Base Budgeting Into Focus." Managerial Planning, Vol. 29, No. 24, March/April 1981.

Wood, Nat. "Rx for Loss Prevention." Security World, Vol. 16, No. 8, August, 1979.

Publications of Government Agencies and Professional Organizations

American Society for Industrial Security. A Selected Bibliography of Security and Loss Prevention. Washington, D.C.: ASIS Publishing Office.

American Society for Industrial Security. Health Care Security. Washington, D.C.: ASIS Publishing Office.

American Society for Industrial Security. Physical Security and Safety. Washington, D.C.: ASIS Publishing Office.

Department of Commerce. "Health Care Services." Crime in Service Industries. Washington, D.C.: U.S. Government Printing Office, 1977, p. 65 - 72.

National Advisory Committee on Criminal Justice Standards and Goals. Private Security: Report of the Task Force on Private Security. Washington, D.C.: Government Printing Office, 1976.

Theses, Research Publications and Other Papers

Buikema, Charles A. "A Survey and Comparison of Private Security Service Legislation in Force in 1981." A Masters Thesis, School of Criminal Justice, Michigan State University, 1981.

Clark, John P. and Richard C. Hollinger. "Theft by Employees in Work Organizations." Minneapolis: University of Minnesota, 1981.

Sherman, Lawrence W. "Learning What Works: A Draft Research Agenda on the Effectiveness and Adequacy of Security on Public Premises." A paper presented at the Conference on Security and Liability at the University of Maryland, 1984.

Sherman, Lawrence W. "Protecting Customers From Crime: Draft Standards with Commentary for Determining the Foreseeability of Crime and the Adequacy of Security on Premises Open to the Public." Washington, D.C.: Crime Control Research Corporation, 1984.

Sherman, Lawrence W. and Jody Klein. "Major Lawsuits Over Crime and Security: Trends and Patterns, 1958-1982." College Park, MD: University of Maryland, 1984.

Sower, Christopher. "Increasing the Effectiveness of Development Organizations." A paper presented at the Asian Regional Seminar on Increasing Effectiveness of Development Organizations, 1980.