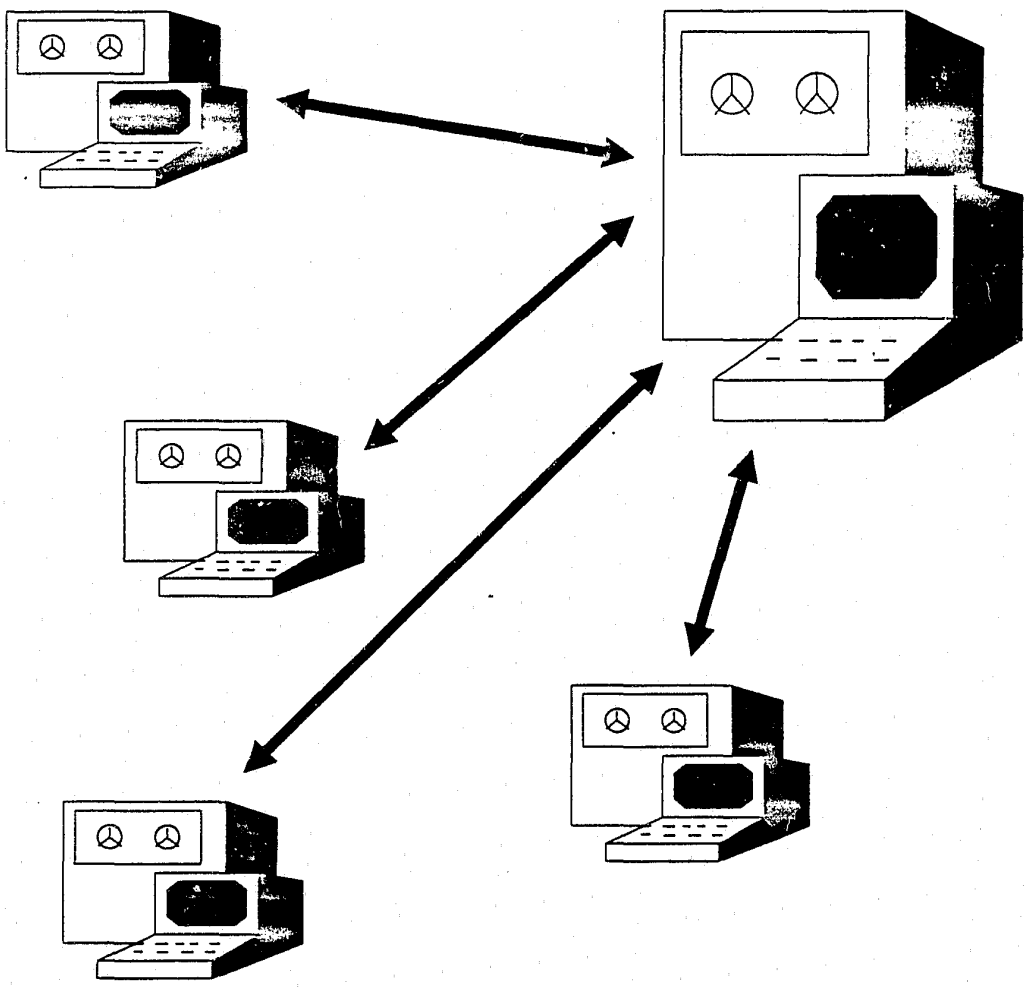
California Law Enforcement

Criminal Information Systems Networking By The Year 2000



An Independent Study by
A. Nicholas Katzenstien
Santa Barbara Police Department
California Command College Class 11 - 0205

This Command College Independent Study Project is a FUTURES study of a particular emerging issue in law enforcement. Its purpose is NOT to predict the future, but rather to project a number of possible scenarios for strategic planning consideration.

Defining the future differs from analyzing the past because the future has not yet happened. In this project, useful alternatives have been formulated systematically so that the planner can respond to a range of possible future environments.

Managing the future means influencing the future--creating it, constraining it, adapting to it. A futures study points the way.

The views and conclusions expressed in this Command College project are those of the author and are not necessarily those of the Commission on Peace Officer Standards and Training (POST).

CALIFORNIA LAW ENFORCEMENT CRIMINAL INFORMATION SYSTEMS NETWORKING BY THE YEAR 2000.

A. Katzenstein. Sponsoring Agency: California Commission on Peace Officer Standards and Training. 1990. 73 p.p.
AVAILABILITY: Commission on POST, Center for Executive Development, 1601 Alhambra Blvd., Sacramento, CA 95816-7053.
Single copies free; order number 11-0205. National Institute of Justice/NCIRS Microfiche Program, Box 6000, Rockville, MD 20850.
Microfiche Free, Microfiche Number NCJ_____

ABSTRACT

The study examines the feasibility of California Law Enforcement Information Systems Networking by the Year 2000. The author reviewed relevant literature, conducted statewide interviews, used the Nominal Group Technique, examined Trends and Events, developed alternative future scenarios, suggests policies and strategic and transitional management plans. Analysis suggests that technological advances will be in place to support a statewide system. The cost of this technology should not outweigh the benefits gained through successful investigations. Public support and a cooperative effort by law enforcement agencies are examined as major social and political issues impacting the networking system of law enforcement information. This study is intended to provide law enforcement decision makers information to consider in the development of their own information systems and the feasibility of statewide networking. Included are Trend and Event Identification and Evaluation; Forecasts; Graphs; Appendices; References.

TABLE OF CONTENTS

CALIFORNIA LAW ENFORCEMENT CRIMINAL INFORMATION SYSTEMS NETWORKING BY THE YEAR 2000

by
A. N. Katzenstein
Commission on P.O.S.T.
Order Number 11-0205

This study examines the factors that will have an impact on the feasibility of a statewide system of California law enforcement information networking by the Year 2000.

Sub-issues are identified as technological advances, the cost and funding sources available , public support for such a system, and law enforcement support for information networking. The study is divided into three parts.

Part One - Futures Study: Utilizing the Nominal Group Technique, several trends and events were identified that impact the issue and sub-issues. The trends that were most significant to the Nominal Group include the level of demand by law enforcement for computerized crime information; the willingness by the general public to support police sharing information; the willingness by the police to learn and use automation; demands by the public to solve crimes economically; and legal mandates for the collection and sharing of information. Significant events were identified as computer terminals being available on every desk and in every police vehicle; a technological advance to link different systems; state funding for seventy-five percent of the networking system; the state mandating uniform crime reports; and all departments becoming "paperless".

Having identified these trends and events an analysis was made to examine the levels of the trends, the probability of the events occurring within the time period being studied, and the impact on the trends should the event occur.

From this information, three scenarios were developed along with policy considerations to support the desired future state.
Part Two - Strategic Management Plan: From information learned in Part One, the creation of Mission Statements, and a situational analysis, six specific policies were developed. They are as follows:

1. Identify the types of reports, or information, that is necessary to share with different agencies. Develop report formats and use abbreviations that are standardized.

2. Public support should be developed and maintained.

3. Develop controls to the access of information and methods to provide for audits.

4. Hire, develop, and retain qualified personnel. Train top level managers in information systems.

5. Develop funding methods to provide assistance to all California Police Agencies.

This part concludes with a recommended strategy to support a statewide system of networking. It also highlights action steps to accomplish it.

Part Three - Transition Management: A project manager was identified as the best alternative structure for managing the transition. The project manager will work closely with representatives of the critical mass to accomplish the organizations goals. The critical mass includes law enforcement managers, investigators, information systems managers, chiefs and sheriffs, technical support personnel, legislative advisors, and a citizens group.

Together this group is responsible for obtaining the necessary support from all stakeholders, and guiding us to the desired State of California Law Enforcement Information Systems Networking.

INTRODUCTION

INTRODUCTION

As we approach the twenty-first century, law enforcement agencies are taking advantage of the rapid growth of information systems technology to more efficiently and effectively conduct criminal investigations. It is imperative, in a highly mobile society, that speed and accuracy of information be provided to police investigators. Modern and future methods of technology are the answer to information exchange.

> Technology is advancing so rapidly that the field of information management - once clouded in obscurity - has achieved a position of primary importance in just a few decades. One thing is certain: complacency will not be coddled. Police executives and agencies of all sizes must keep abreast of this technology if they are to continue to deliver the sophisticated services demanded today. (Cameron, 1990)

Almost all California Law Enforcement agencies have developed an automated Records Management System (RMS). Typically, these are files to index information related to crime reports, traffic incidents, property and evidence bookings, arrest reports, and field interviews.

More sophisticated systems provide for crime linking utilities, crime analysis forecasting of criminal activity, and investigative caseload management for investigators.

During the development of these programs most departments focused on their individual needs. Crime information was reported using local report formats and entered into RMS in a manner each jurisdiction believed would suit their individual agency's needs. The time has come, however, that police departments are recognizing they are on the edge of needing systems of local networking, in addition to state and national, for information to solve criminal investigations. With all of the innovations in computers and software, simplifying police work in the office has rapidly become

not only a reality, but a necessity. Police departments are continually investigating the options available in computer systems, and, according to Condon (William Condon, an Account Representative at Wang), law enforcement sales are the number one opportunity in the local government market. "It is the thing to do for police departments". (Shaw, 1989)

> Computer literacy is on the rise in law enforcement agencies, and most departments are now very interested in computerization. However, even if the police department wants to join the computer age, the city or county is still usually the one governing the budget. Therefore, computer industry experts realize the need to highlight a product that can offer the most benefits and grow with the size of the department.
>
> Due to the growing needs within the market, law enforcement agencies can expect to see continual changes, updates and expansions in computers and software. (Shaw, 1989)

The most sophisticated criminal information networking system in California today is the California Law Enforcement Telecommunications System (C.L.E.T.S.). Thirteen main computer switching stations, located throughout the state, serve to link more than 2300 independent terminals to criminal information files with the State Department of Justice. This system also allows agencies to network with the National Crime Information Center for National and some international crime information. C.L.E.T.S. also has the capability of networking with other states for limited information, such as drivers license history, vehicle registration, and criminal history.

Cities and counties within the state have traditionally relied on these state and national systems to provide them with crime information related to wanted persons, missing persons, unidentified persons and vehicle and other property thefts. Investigators have also used these files, in the course of backgrounds, to track the Department of Motor Vehicle information and criminal history on their suspects.

> As most criminal justice practitioners are aware, NCIC was established by the FBI in January 1967 to provide a nationwide, user-oriented, computer-based, inquiry/response information system available 24-hours per day to all local, state and federal criminal justice agencies through a telecommunications network. Documented criminal justice information is stored on-line at FBI Headquarters in Washington, D.C. and made available upon authorized request for wanted, missing and unidentified persons; stolen and felony vehicles; stolen vehicle parts; stolen license plates; stolen and recovered guns; stolen boats; stolen securities; and other stolen articles. It also provides an index of criminal histories and maintains information on extraditable foreign warrants. A file of individuals who have made threats against the President of the United States and other certain public officials under U. S. Secret Service Protection is maintained as a locator service to that agency. Currently, the NCIC Data Base, which exceeds twenty million records, is queried by 59,362 authorized users who are conducting as many as one million transactions per day (an average of over eleven transactions per second). The Wanted Person file contains 335,000 subjects". (Netmeck, 1990)

Research has shown that there has been some effort to regionalize police records information networking in some areas within the state. This has come about with the realization that local agencies collect crime information on offenses and suspects that with systems networking can provide other agencies with more timely information to identify suspects and solve crimes.

One of the earlier systems developed in the 1970's, among a group of police agencies in the Los Angeles County area, is known as the Leader System or Law Enforcement Automated Data Entry and Retrieval System. This system not only allowed for automated records within individual agencies but networked those, who chose to participate, with neighboring agencies for information pertaining to crimes and incidents, arrests and bookings, field interviews, traffic accidents, traffic citations, and data regarding registrants and applicants. This local information is not normally available at the state or federal level and has proven to be valuable to the investigative users.

San Diego County has also developed a system known as ARJIS, the Automated Regional Justice Information System. This system is comprised of nine major components. These interacting components correlate regional information concerning the identification of individuals and how they are known to the law enforcement community. Each of the regional police agencies in San Diego County has one or more terminals which allow on-line access for either inquiry or update activity on arrests and juvenile contacts, automated worthless document index, citations, crime analysis, crime cases, field interviews, master operations index, personnel, and pawned or wanted property. This too, has proven to be effective for the San Diego area users.

Other areas within the state have also begun work on local area networking. The counties of Kern, Marin and San Joaquin are jointly developing an integrated criminal justice information system.

Law enforcement agencies in the County of Riverside have shown interest recently and participated in a study to identify agency requirements and existing information systems county wide. In a draft report produced in June 1990, it is evident that these agencies are looking for a county wide system to network their information.

From the field officer to the highly trained investigator other agency information is invaluable. The criminal element has never realized jurisdictional boundaries, yet police officers have had to conduct their business under the limitations imposed by local collection, storage, and access to information. To seek information from other agencies is often frustrating and time consuming through the traditional means of personal contact or telephone communications.

The purpose of this study is to examine the issue of statewide law enforcement information systems networking. Trends and forecasted

events will be analyzed to project where the issue should and/or will be by the year 2000. Strategic plans will be developed and a transition management program established to attain the desired future state of information systems networking.

FUTURES STUDY

ISSUE

What will the state-wide feasibility of California Law Enforcement Information Systems Networking for criminal investigations be by the year 2000?

SUB-ISSUES

I. How will technological advances support the number of users considering the quantity of data and urgency of need?

II. How will the cost of technology impact the issue?

a. What alternatives will be available to traditional funding?
b. Will state and federal government assist cities and counties in funding?

III. What will be the level of support by the public for police data gathering and sharing?

a. How will access to information be controlled?
b. How will the concern for public safety weigh against the concern for individual privacy?

IV. Will police management support information sharing considering the potential for liability.

DEFINING THE FUTURE

NOMINAL GROUP TECHNIQUE (NGT)

To examine this issue and sub-issues, seven persons with backgrounds in computer science, police records management, laws related to law enforcement information, and criminal investigations were brought together to employ the NGT. They initially identified thirty-five trends and twenty-three events that impact the issue. These trends and events were eventually rank ordered to select the five thought most significant by the Nominal Group.

TRENDS

1. Demand by law enforcement for computerized crime information - The level of value to having computerized crime information available to officers on a regional or statewide system.

2. The level of willingness by the general public to support data banks to control crime - Public support, with regard to privacy issues, for police computer systems.

3. Willingness by the police to learn and use automation - Support for the use of regional data banks by both police management and line officers.

4. Demands by the public to solve crimes economically - The public response to capital outlay versus the return through successful investigations.

5. Legal mandates for the collection and sharing of information - Will there be more requirements or less from our legislative and judicial branches of government?

TREND EVALUATION

Note: The following evaluations contain panel median forecasts. For range, please refer to the Trend Graphics in the Appendices.

1. Demand by Law Enforcement for computerized Crime Information.

   The group felt that this demand has increased by 40% in the last five years. This is a reflection of a more computer literate police force, the mobility of criminal suspects, and efforts being made at the federal (NCIC 2000), state (Cal ID), and local (Limited LAN's) levels to develop advanced programs. They view what they believe "will be" a rate of increase in this trend to be to 50% by 1995 and 80% by the year 2000.

   In their preferred future, they believed the level of this trend should be much higher, increasing by 300% in five years and 400% in ten years. Most of the discussion related to this wide range centered around the lack of management support for the necessary program development and financial commitment needed by cities and counties.

2. The level of willingness of the general public to support data banks to control crime.

   The group believes that because of increased crime rates, an influx into our society of both legal and illegal aliens, continued international drug smuggling, and a public outcry for "quality of life", that there will be increased public support of this trend. They see this support as having increased by 40% in the last five years. They believe it will increase to 50% in five years and to 130% in ten years. In the "should be" forecast the level increased by 300% in five years to

400% in ten years. This is best explained by a feeling that the general public will be slower in responding the value of police data banks than the criminal justice professionals who participated on the panel.

3. Willingness of the police to learn and use automation -

The level of this trend is viewed as having increased by 50% in the last five years. The group sees an additional 50% increase by 1995 and a more accelerated use by 200% in the year 2000.

There has been moderate response to police computer systems as pre-computer law enforcement officers in the waning years of their careers are being mixed with computer literate young officers of today. By 1995, most managers and all officers will have received formal training in systems and use of computer programs. In the "should be" future state this would have increased by 300% in 1995 and 450% by 2000.

4. Demands by the public to solve crimes economically -

Always looking to get the "best bang for their buck", community leaders, representing their constituents, have begun to appreciate the value of computer programming that networks law enforcement information. NCIC has had many notable successes, particularly with missing persons. Serial murder cases crossing multiple jurisdictions have been solved through information systems networking. Today's media has portrayed these successes throughout the public. Although the start up costs have been expensive, advances in technology should drive prices down making systems even more economical compared to traditional investigative means.

The trend level is viewed as having increased by 50% in the last five years. It will increase by 100% in five years and 300% in ten years. The group thinks it should increase by 300% in five to 400% in ten years.

5. Legal mandates for the collection and sharing of information -

The group sees this trend as having increased by 50% in the last five years. This is a continuation of legislative efforts to identify found bodies, track child and spousal abuse cases, locate missing persons, and identify criminal offenders. This trend will increase by 40% in five years to 200% in ten years. This increase is explained through expectations of successes with Cal-ID, DNA, data banks on known serious offenders and early release programs from overcrowded jails and prisons. This "should be" increased by 100% in five years and 200% in ten years. The feeling is that the legislators will cautiously balance "right to privacy" with information collection.

EVENTS

Of the twenty-three events identified by the Nominal Group Panel, they selected five that they believed would significantly impact the issue were they to occur during the period of time being studied.

During the exercise they completed event evaluation forms to forecast the number of years until the probability of the event occurring first exceeded zero, and the probability of its occurrence five and ten years from now. The panel then rated its positive or negative impact should the event occur. It should be noted, that of the selected events, the panel found no negative impact on the issue if they were to occur.

E1. Computer terminals are on every desk and in every police vehicle -

The panel median believed we were at least five years away from any probability of this occurring. In five years from now, the median found a 50% probability and in ten years a 90% probability.

The panel ranged from three years to the event first exceeding zero to the probability of it having no chance to occur until 1999.

It was given a 70% chance to occur by the year 2000 and the lowest range and a 100% chance in the highest forecast of ranges.
Economics and fiscal planning for capital programs was the greatest influence on the panels median forecast and range.

This event was seen to have an extremely positive effect on the issue. The Group believes that with more available terminals, and increased frequency of use, that users will better recognize the value of systems networking.

E2. A technological breakthrough occurs to link different hardware systems together.

The panel median forecasted that we were at least four years from the probability of this occurring. They believed that in five years there will be a 50% chance of occurrence and in ten years a 100% chance. The lowest forecast was 50% by the year 2000, but was an isolated forecast. Both the median and high range forecasts are to 100% probability by 2000.

The group considered cost factors when identifying and considering this event. It is possible, today in 1990, for technology to link different systems. The cost factor is, however, prohibitive. As the cost of technology, both for programs and methods of transmission is reduced, the probability of this event occurring is increased. This breakthrough resolves a major drawback to networking today and is seen as having the highest (10) impact on the evaluation scale for the issue.

E3. The State Department of Justice develops a program to pay for 75% of local police computer systems.

A major alternative to individual department budgeting would be for the state to finance a portion of systems equipment. This funding could cover costs of hardware, software, communications lines, and maintenance.
The median sees this as having its first opportunity of occurrence in five years yet sees the probability at 50%. Its probability of occurrence by 2000 is 80%. The low range indicates a probability of 50% in five years.

The high range is 100% in ten years. This event also carries an extremely positive (10) effect on the issue area. It should resolve the fiscal concerns of all departments in the state.

E4. State mandates automated uniformed crime reports.

The group did not see a probability, beyond zero, of this event until five years from now. At that point the probability immediately rose to 50% and then to 100% in ten years. The low range of probability was 50% by the year 2000, but once again this was an isolated forecast.
This event would have a positive (7) impact on

networking. It would contribute to agencies speaking the "same language" on crime information reporting.

E5. All departments become "paperless".

The first year this event could occur was projected to be 1995. Its probability, according to the Panel Median, is 50% at that time, and 80% by 2000. The low range of its probability by 2000 is 50%. The high range is 100%. This event also carried a positive (5) impact on the issue. As our systems of information storage become more technologically advanced so will our systems of accessing this information.

CROSS IMPACT EVALUATION

A cross impact matrix was used to do an evaluation to gauge the effect that each event would have on other events and our candidate trends. In this table the numbers reflect a positive percentage impact should the event actually occur. By focusing our attention on actor events (those having the most influence on other events and trends), we can better prepare ourselves for policy considerations that are most influential to our issue of information systems networking.

E1. Computer terminals on every desk and in all police vehicles.

This event is more of a reactor than actor. It would have some minimal influence on uniform crime reporting. It would have a tremendous positive impact on the probability of paperless police departments. It would also have a positive impact on each of the trends with the exception of legal mandates which it is viewed as having no impact.

E2. Technological breakthrough to link systems. This is an actor event that influences all other events and trends. It is a "gateway" event that would be the foundation for systems networking.

E3. DOJ program to pay for 75% of police computer systems. This event also has positive impacts on all other trends and events with the exception of the technological breakthrough. The positive impact is so high that consideration should be given to influencing state government to fund a portion, if not all, that is identified in this event.

E4. State mandates automated uniformed crime reports.

This event would have a positive effect on increasing support for most all of the trends. It becomes a "foundation event" for systems networking, absent a cooperative effort at the local area. The group did feel that it may not directly impact the trend of the demand of the public to solve crimes economically. This event is viewed as also having no impact on other events except for paperless police departments. It is a "stepping stone" for paperless agencies.

E5. All police departments become "paperless". This event impacts, and virtually necessitates, computer terminals on every desk and in all police vehicles. It also impacts, to a degree, the fiscal support of the state. The event has a positive effect on all trends.

SCENARIOS

A scenario is a non-fictional narrative which presents a set of forecasts in such a way that causes and consequences of major forecasted changes are clarified and the narrative as a whole facilitates the identification and evaluation of relevant polices or actions by the user.

NOMINAL SCENARIO

The nominal scenario is based upon the forecasting groups "will be" trend projects. None of the forecasted events occur.

January, 2000:

The turn of the century has brought with it many technological advancements in law enforcement. We are in an age of non-lethal weapons, advanced radio communications, and "smart" highway systems.

One area that we have fallen behind in, is local information systems networking for criminal investigations.

Early efforts of the 1980's by law enforcement to computerize their crime information slowed dramatically during the 1990's. Once local systems were developed they tended to focus on the needs of individual departments. Little or no effort was made to explore the benefit of having access to other departments crime data banks. In part, this was due to rather apathetic support from the public. They still had major concerns about information, often times personal, being available to law enforcement outside their own communities. The fear of "big brother" still lingered, to a degree, some sixteen years after "1984".

Another public support factor has been economics. Having barely survived a long period of increased income taxes, escalating medical costs, and user fees for just about anything outside of the basic necessities, the public through its political representation, has been hesitant to support capital programs, regardless of long term benefits.

Although computer literacy exists throughout the ranks of law enforcement, this lack of public support has caused little interest in the program development needed to integrate systems.

There has been very little movement at the state level to mandate the collection and sharing of law enforcement information. What has been done is limited to satisfying federal requirements and those of special interest groups who have succeeded in lobbying their representatives. The legislative attitude has been one of re-actionary.

NORMATIVE SCENARIO

The normative scenario concentrates on the "should be" trend data. These trends are supported by all five of the forecasted events in

that each has a positive impact on the issue. The setting for this scenario is the Annual Robbery Investigators Association meeting in Sacramento; Year 2000. A presentation is being made by Sgt. Griffith, a Fresno Robbery Investigator.

Ladies and gentlemen, it is with great pleasure that I have been given this opportunity to share with you the successful conclusion of a series of robbery cases that have occurred during the last three months in the Fresno County area.

As you may have heard, a team of three robbery suspects appeared to be responsible for fifteen jewelry store robberies. In each case, they wore gloves and masks. Other than general height and weight descriptions, the only personal identifier was a tattoo on the left forearm of one of the suspects that said "Saigon 1971". This tattoo was observed by victims in five of the robberies. In addition, a grey Chevrolet was seen in two of the cases. In one of these, a partial license plate beginning with AZ was taken by a witness. After checking with informants, putting out local be on the lookouts and exhausting inquiries into local police data banks for suspects with similarities, it appeared these suspects were from elsewhere; contrary to what an unreliable informant had previously led our investigators to believe.

I can remember when I first came to Robbery in the late 1980's. Back then our investigation would have come to a standstill. Sure, we would have shared our cases with other departments, through teletype, telephone contacts, or mail-outs, but seldom did we solve cases like this. We usually waited for them to hit again, using several detectives and many hours of overtime on stakeouts.
Thanks to proper planning, cooperative efforts by policing agencies, technological advances, and support by the public, we solved these cases with today's capability of information systems networking.

One of our investigative teams was assigned to work at their desks

doing inquiries into county and city data bases for arrest information on persons with tattoos, and traffic citation records on grey Chevrolets with the partial license of AZ.

Following a search late one evening, one of our investigators found a match on the general description and tattoo of a person from the records of the Santa Barbara Sheriff's Department. That same evening, they found that the Santa Maria Police Department had issued a citation to the driver of a grey Chevrolet with the license plate of AZD997.

The following morning, criminal history checks were made on both persons. We learned that they had both served time in the Lompoc Federal Prison together. Their crimes ranged from assault to narcotic violations and robbery. Both were also on parole.
We then made arrangements with their parole officers to conduct similtaneous parole searches at their two different places of residence. Not only were we successful in locating evidence from four of our cases and the Chevrolet, but we found the brother of one of the suspects who admitted to being the third party involved in the robberies.

Once again, I cannot see this case as having been so successfully resolved without our Law Enforcement Information Systems Networking of today. I encourage all of you to take advantage of it, and don't put so much stock in the information of an unreliable informant!

HYPOTHETICAL SCENARIO

The hypothetical scenario describes the trends and events, as if they had occurred. In this case, we will explore how improper planning and transition management allowed for a turbulent future.

January 1990

With much frustration, Sergeant Schmidt sits behind his desk reviewing the previous day's robbery reports on his terminal. Thinking about efforts of the early 90's to develop law enforcement computer systems and networking them with other agencies is the source of his frustration.

Rushing into the world of Automated Records Systems, Police Departments with funding from the Department of Justice, rapidly went out and purchased hardware and software programs with very little thought given to the needs of the working detective to access other agency's information systems.

Sure, today's technology has an answer to the mechanics of this problem but many others have stifled previous efforts to have a workable system. When the state tried to mandate uniform crime reports no care was taken to address concerns of both rural and urban areas. Likewise, with our multi-culture population, little care was taken to clarify differences in national origin. As a result, the most popular box to check in many categories of crime reports is "other". "Garbage in, garbage out' mutters Sergeant Schmidt, thinking aloud.

Other areas of failure include public and political support for the collection and sharing of crime data. Frustrated with drug abuse, concern for missing persons, early release of convicts, and an overall increase in serious crime, law enforcement had the initial support of the public.

A failure to share some early successes, coupled with several cases of individual officer abuses of access to information, has not only diminished public and political support, but has police management "running scared" of liability issues. The attitude of today is that if the information cannot be substantiated by two or more independent sources, don't record it.

Once more, Sergeant Schmidt sighs, "if only I had been a part of the planning and implementation process".

POLICY CONSIDERATIONS

The Normative Scenario offers the most desireable state given the objective stated by the issue. Consequently, the impediments to achieving the objective of networking can be mitigated.

A method to accomplish this goal is to develop initial policies for consideration.

Initial Policy Alternatives

1. Investigators are crying out for support in helping them solve multi-jurisdictional crimes. Police departments should focus their attention to this need.

2. Further develop community support. Departments should share, through all media sources, crime information on multi-jurisdictional offenses. Community presentations should highlight these problems and solutions.

3. Mitigate public concerns related to misuse of information. Develop training programs within departments to address criminal and civil liabilities of unlawful computer usage.

4. Hire computer literate employees. Departments should consider computer literacy in their recruitment and selection process.

5. Sell the public on the economic value of networking technology. Present cost comparison data at community forums.

6. Sell the legislative body on the economic value of networking and its potential for crime solution. Enlist the assistance of PORAC, Cal Chiefs, CAL Sheriffs and other influential bodies for this effort.

7. Identify user needs to our different vendors. Rather than working with what is available, dictate future needs for vendor research and development.

8. Coordinate efforts by all agencies to satisfy needs of information collection. Develop like entry data.

9. Identify which information should be accessed by outside agencies and which should be restricted.

10. Capitalize on funding programs, other than tradition budgeting, for financial assistance, i.e. drug asset forfeiture, grant programs, penalty assessments, user fees, etc.

11. Educate top level law enforcement managers to the value of information technology enabling them to improve services to the public and reduce the cost of service delivery.

STRATEGIC MANAGEMENT PLAN

STRATEGIC MANAGEMENT

A Strategic Plan for California Law Enforcement Criminal Information Systems Networking

In order to facilitate the desired future state for California Law Enforcement Criminal Information Systems Networking, we now step into the planning process.

The model for this plan is a variation of the existing California Law Enforcement Telecommunications System. At present, CLETS acts to receive inquiries from users, and disburse information stored in central data banks within the Department of Justice. It also acts as a switching station to access central data banks in other states and the Federal Records of the National Crime Information Center.

The variation is that CLETS would serve as a switching station for all California Law Enforcement agencies to interact with one another. The role is referred to as being a "mail router". Beyond this model, the application of this plan is envisioned to, one day, extend to the federal and international levels of law enforcement.

MISSION STATEMENT

No planning should proceed without a Mission Statement to lay a foundation for strategies and decisions, build commitment, and insure consistency.

The following statements have been developed for our model organization.

MACRO-MISSION

The mission of law enforcement is to protect the right of all persons to be free from criminal attack, to be secure in their possessions, to live in peace and to service the public by performing the law enforcement function in an efficient and professional manner.

MICRO-MISSION

We must be responsive to new technology and all law enforcement agencies must work together in the sharing of information that may lead to the solution of crime and the arrest of offenders throughout all jurisdictions of the State of California.

SITUATIONAL ANALYSIS

A technique used to analyze our situation is referred to as the WOTS UP analysis. WOTS UP is an acronym for weaknesses, opportunities, threats, and strengths. The WOTS UP analysis helps to determine whether the organization is able to deal with its environment. This technique allows us to view the external enviornment by identifying opportunities and threats. We then view our internal enviornment by identifying our strengths and weaknesses. This then leads to underlying planning which is involved in policy implementation.

Opportunities

1. The public is interested in their safety and the protection of their property.

2. The judicial branch of government has become more conservative in it findings related to constitutional issues of public protection.

3. There are national efforts in support of better and faster law enforcement information exchange.

4. Media coverage has brought the issue of multi-jurisdictional crimes to the attention of many more people.

5. As technology has advanced, systems have become less expensive.

6. Laws are being established to assist law enforcement with funding for crime reduction.

7. New methods to increase data storage are being developed.

Threats

1. The American Civil Liberties Union will oppose information exchange both in the courts and through the media. There is still a perceived concern about "Big Brother".

2. The spending limitations imposed on government will make it difficult for some cities and counties to find funding.

3. Political economic concerns may divert funding from the Department of Justice.

Strengths

1. Today's officers are more computer literate and will support changing to systems networking.

2. POST is funding training programs in computer literacy.

3. Competition between agencies is diminishing and they are becoming more supportive in others efforts to solve crimes.

4. Crime Analysis programs are being implemented in more and more departments.

5. Departments are hiring more data processing support personnel.

Weaknesses

1. Many departments have invested in systems that will not be compatiable to networking.

2. Many upper and mid-level managers have no computer background.

3. There has been several cases of unlawful use of information within agencies.

4. Departments have different report formats, usually to satisfy their perceived individual needs.

STRATEGIC ASSUMPTION SURFACING TECHNIQUE (SAST)

SAST is a method used to identify stakeholders and their relation to the strategic issue being addressed. Stakeholders are individuals and groups or organizations who: 1) are impacted by what the organization does; 2) are able to impact the organization; or 3) are concerned about the issue and/or the organization.

1. The Governor
2. The State Attorney General
3. Legislators
4. County Sheriffs and Police Chiefs
5. Police Middle Management
6. Investigators
7. Crime Victims
8. District Attorneys
9. Information Systems Managers
10. Communications Vendors
11. Media (Snail Darter)
12. Defense Attorneys (Snail Darter)
13. American Civil Liberties Union (Snail Darter)
14. Information Systems Software Vendors
15. City and County Attorneys
16. Citizen's Advisory Group

Stakeholder Assumptions

The following is a list of assumptions made about each of the stakeholders related to the issue area.

The Governor

1. Is interested in the delivery of high quality of law enforcement services.

2. Will support legislative efforts to find funding for systems networking.

The State Attorney General

1. Will support statewide systems networking.

2. Will develop guidelines for the use and security of the network.

3. Will assist agencies in the investigation of security violations.

Legislators

1. Will generally support a networking program.

2. Will be cautious about funding.

3. May futher develop legislation to allow for additional seizures of property obtained illegally.

4. Will be concerned about security violations.

County Sheriffs and Police Chiefs

1. Will be hesitant about allowing personnel from outside their agencies to access their records.

2. Will demand the ability to conduct internal audits.

3. Will look for assistance with funding.

Police Middle Management

1. Will be willing to coordinate efforts with other

agencies.

2. Will be creative in funding efforts.

3. Will support needs of information systems managers in working with systems vendors.

4. Will support investigators needs.

Investigators

1. Will learn and use the network system.

2. Will share their successes with others.

3. Will be more attentive to detail in their reports.

Crime Victims

1. Will bring pressure on their legislators to support funding.

2. Will make additional demands on law enforcement to solve criminal acts.

District Attorneys

1. Will support a networking system.

2. Will want to become a part of the system to assist in their own investigations.

Information Systems Managers

1. Will take an active role in the development of the

program.

2. Will probably demand more staff assistance.

3. Will be conscience of security issues.

Communications Vendors

1. Will develop communications lines to support and maintain the system.

Media

1. Will give negative press to any security violations or errors in the system.

2. May cooperate with positive reports on successful multi-jurisdictional investigations.

Defense Attorneys

1. Will capitalize on any system errors that lead to misinformation.

American Civil Liberties Union

1. Will object to the system from the onset.

2. Will try and fight the networking in court.

3. Will use the media to fight the program.

Information Systems Software Vendors

1. Will work with law enforcement to develop the programs.
2. Will develop newer and faster systems.

City and County Attorneys

1. Will have concerns about liability.

2. Will insist on limitations to the type of information being released.

Citizen's Advisory Group

1. Will have mixed concerns on privacy issues versus law enforcement data collection and dissemination.

2. Will influence the legislative body of the state.

POLICY ALTERNATIVES

Having examined, through the WOTS-UP analysis and strategic assumption surfacing technique, our issue related to the environment and stakeholders, we are able to develop policy alternatives.

1. Law enforcement agencies should develop their systems now for the future of networking.

2. The public should be kept appraised as to the significant value of systems networking.

3. The State of California should be monitoring federal efforts in networking.

4. Recruitment efforts should focus on computer literate personnel.

5. Existing personnel and police managers should receive training they may have missed in their formal or professional educations.

6. Reports that would be of value to other agencies, as well as those, that should remain internal, need to be identified.

7. Report formats need to be standardized.

8. Hardware and software providers must be brought into the goals of the organization.

9. Establish inter-agency planning groups to move statewide efforts toward networking.

10. Work with the leglislature to develop additional sources of funding.

11. Develop security standards to address concerns of misuse of information.

12. Adopt approved communications protocols.

13. Seek federal funding assistance.

MODIFIED POLICY DELPHI

The Modified Policy Delphi is a process designed to examine policy issues. A policy issue is defined as an issue for which rational individuals advocate differing resolutions. The Policy Delphi is designed to; 1) generate strategic alternative approaches to the policy issue, 2) analyze the feasibility and desirability of each alternative, and 3) reduce the number of alternatives to a manageable number for more complete strategic analysis.

A Policy Planning Group consisting of law enforcement managers, managers of law enforcement information systems, and systems analysts were asked to evaluate the various policy alternatives for both feasibility and desirability. In the final analysis, six policies were identified for assessment.

Policy One: The organization should identify the specific reports that will be made available to different departments. Report formats should be the same. Abbreviations should be standardized.

Pros:

1. This will allow agencies to share necessary reports yet protect those that should remain internal to a department.

2. Like formats will capture like data and not confuse the user.

3. As in Number 2, the user will not be as likely to misunderstand the data.

Cons:

1. Some users may believe they could do better with total access to information.

2. Some departments may feel a generic report will not satisfy their data collection needs.

3. Training will be required in the use of new report forms and abbreviations.

Policy Two: Public support should be developed and maintained. Without this support, social and political ramifications could lead to defeat of the system.

Pros:

1. Public awareness will minimize fear of the misuse of information.

2. The sharing of successes will lead to financial support to develop and maintain the system.

Cons:

1. The media may reverse public support should violations occur.

2. Vocal groups will develop to suggest law enforcement is focusing on minorities or individuals.

3. The American Civil Liberties Union will argue on a public forum.

Policy Three: Information security. Increased access to statewide data bases places a higher priority on computer security. The system needs to be developed to provide for appropriate access and necessary audit of users.

Pros:

1. This will minimize misuse of information.

2. This will provide for a system to identify violations.

Cons:

1. It will increase the workload to those charged with the responsibility of conducting audits.

2. It will bring violations to the attention of the media and the public.

3. It will no doubt lead to the identification and dismissal of violators.

Policy Four: Hire, develop, and retain qualified personnel. Train top level managers in information systems.

Pros:

1. This will avoid the under use of technological resources.

2. This will allow management to better understand the use of technology to improve service and reduce the cost of service delivery.

Cons:

1. There will be much competition from both the public and private sectors for these qualified personnel.

2. Training for management level personnel will be viewed as costly.

Policy Five: Develop funding methods to provide assistance to all California Police Agencies. Seek legislative aid to enhance the seizure of property and have its value returned in the fight against crime.

Pros:

1. This will provide funding that may not be available to agencies through the traditional budget process.

2. It will provide for the update of new and better system as they become available.

Cons:

1. It will be viewed by many as the misuse or excess of government authority.

2. It may bog down the court system with legal challenges.

Policy Six: Establish inter-agency planning groups of information managers, and law enforcement managers and investigators to monitor and further develop the systems network.

Pros:

1. This will provide an opportunity to keep current with technological advances.

2. The group can work on difficiencies within the system.

Cons:

1. There will be some disagreement within these groups related to individual needs.

2. Costs of travel, accommodations, and time will be important to management.

RECOMMENDED STRATEGY

The State of California should work with law enforcement agencies in an effort to provide for crime information sharing between departments.

The technical issues of data gathering and dissemination need to be evaluated to suit the needs of the different departments. Public support must be attained and retained. Our legislative body, with the support of their constituancy, must assist with the funding of the program.

Qualified personnel must become a part of police agencies from line through staff if we are to meet our commitment to our Mission Statement.

Action Steps:

1. Identify the Transition Management Team.

2. Have this team evaluate the current systems of data collection and dissemination throughout departments, for their technical capabilities of networking.

3. Have them meet with hardware, software, and communications vendors to present plans and develop programs.

4. Approach legislators for funding support.

5. Prepare the public to support the systems network.

6. Work with POST to identify training needs.

7. Recruit information systems and computer literate personnel to provide data processing staff necessary to support the program.

8. Work with the organizations of California Chiefs and Sheriffs to win their support.

Time Line:

Before a time line can be truly established, the management team of the organization must be developed. From this point, support from the public, political, upper management law enforcement personnel, and other stakeholders, should be secured in a one to two year period. In three to five years funding can become established.

With many of these steps either taken or being continuously developed, and with the advancement and reduced costs of new technology the program of a desired future state of law enforcement information systems networking should be in place by the year 2000.

TRANSITION MANAGEMENT PLAN

LAW ENFORCEMENT INFORMATION SYSTEMS NETWORKING FROM 1990 TO 2000

Managing change is one of the most critical elements of any organization's development. It becomes exceptionally difficult, when dealing with a subject such as Law Enforcement Information Systems Networking. We are breaking away from traditional grounds of local agency control, facing concerns about individual privacy, and looking at substantial financial investment. It becomes imperative then, that an effective transition plan be developed, for our organization to be successful.

The Critical Mass

The Critical Mass, an analytic tool for use in transition planning, helps identify those few key people, or groups, who are critical to the success of the strategic plan. The critical mass is the minimum number of stakeholders who if they support the change you are likely to succeed, or if they oppose the change you are likely to fail.

The following stakeholders are identified as being the critical mass for our organization:

The State Attorney General
The State of California Legislators
The County Sheriffs and Police Chiefs
Police Middle Management
Information Systems Managers
The General Public

Readiness/Capability

With this critical mass identified, it now becomes necessary to make assumptions of each person, or group, in terms of their disposition toward the proposed change at this time.

The following chart illustrates assumptions of both readiness and capability.

Actors in the Critical Mass	Readiness Hi	Med	Lo	Capability Hi	Med	Lo
Attorney General		X		X		
State Legislators			X			X
Sheriffs and Chiefs		X		X		
Police Management	X			X		
Information Managers	X			X		
General Public			X			X

Commitment

Having made these assumptions it is necessary to examine the level of commitment required in order for the change to be successful. The following chart identifies the current level of commitment and necessary change for success:

Actors in the Critical Mass	Type of Commitment: Block Change	Let Change Happen	Help Change Happen	Make Change Happen
Attorney General		O		X
State Legislators	O		X	
Sheriffs and Chiefs		O	X	
Police Management		O		X
Information Managers				OX
General Public	O		X	

O = Present X = Change

Influencing the Critical Mass

The Attorney General: As the Chief Law Enforcement Officer of the State of California, the Attorney General must be committed to making change happen. In our organizational model, it is the Department of Justice, that will be the focal point of our message switching system. The Attorney General must provide the technical

making change happen. In our organizational model, it is the Department of Justice, that will be the focal point of our message switching system. The Attorney General must provide the technical support to develop and maintain the system. There must be personnel from the Department of Justice to monitor improved technology to later enhance the system. Investigative personnel must also be available for security violations as they may arise.

State legislators: Initial assumptions of this group reflect a low readiness for change and a block change in their present commitment. State spending has been under scrutiny by the public since the mid 1970's. Different initiatives have been imposed by taxpayers. Legislators have been stressed by financial limitations. This group must be convinced of the value to public safety of law enforcement information systems networking. They must also be creative in enacting legislation to divert criminal enterprise funds back into the hands of law enforcment. They must also answer to their constituency on issues of privacy laws. Both of these areas are sensitive to our legislators. Champions of law enforcement, among them, must be cultivated to influence the others.

Sheriffs and Chiefs: As law enforcement department heads this group must be moved from a let change happen position to help change happen. There will be a significant financial investment that will be viewed as a financial burden on cities and counties. Sheriffs and Chiefs must "buy into" the value of our organization and then "sell it" to their funding sources. They must also be comfortable with the program of security and limited access to their department's information files.

Police Managers: If the organization is to be successful, police managers must be committed to making change happen. Members of this group play a role in the organizing, staffing, and controlling of police organizations. They will be personally responsible for identifying which agency files should be permitted for access by

others, hiring and training needs of supporting staff, and audits to insure security. Department representatives, from this group, will need to participate in county, regional, and/or statewide inter-agency planning groups to resolve problems and further enhance the program.

Information Managers: With a high readiness and high capability, this is the technical group that is ready to make change happen. Research shows, I found that this group is only limited to funding and staffing for technological advances. With support from other members of the critcial mass, they will make the organization happen.

The General Public: This actor in critical mass must be moved from a position of blocking change to a position of letting change happen. As mentioned in other parts of this study, the general public has a serious concern about their safety and security. To this end, they have supported law enforcement much differently than in the 1960's and 1970's.

As international drug problems, gang activities, and other crime matters continue to plague the nation and the state, and be highlighted by the media, their support is expected to continue. This is the time to take advantage of this support and cover a vocal minority with a more safety concerned majority.

MANAGEMENT STRUCTURE

In reviewing alternative structures for managing the tansition from our current state to the desired future State of Law Enforcement Information Systems Networking, it seems most appropriate to have a project manager assigned from the Department of Justice. The project manager, appointed by the Attorney General, would have the authority necessary to mobilize the necessary resources within the Department of Justice and the respect of law enforcement agencies and information systems managers now using C.L.E.T.S.

This person should also possess the interpersonal skills necessary to be persuasive when dealing with the concerns of other stakeholders.

The project manager will lead a task force consisting of representatives of law enforcement managers, investigators, information systems managers, police chiefs and/or sheriffs, technical support personnel, legislative advisors, and a citizens advisory group.

SUPPORTING TECHNOLOGIES

Several methods and tools are available and should be used to better manage the transition.

1. **Responsibility Charting (RASI):** RASI is a mechanism that has been developed and used successfully to clarify role relationships among actors in the critical mass. Having identified different tasks those individuals or groups in the management team agree upon who must be Responsible for a task or decision; who must give Approval with a right to veto; who should Support with no right to veto; and who should only be kept Informed on the matter. See Appendices, p.73.

2. **Team Building:** Through a series of workshops the transition team should develop a clear understanding of the concept and develop a commitment to making the plan a success.

3. **Problem Finding:** Each committee in the transition team will find problems inherant to their area of responsibility. Often times these problems will overlap into another area. Again, a series of workshops will be conducted to resolve these issues.

4. **Communication Strategy:** The project manager will arrange

for communications throughout the law enforcement community, within the actors in critical mass, and to the general public.

5. **Helping Departments Let Go of the Old:** The project manager must be alert to those who may attempt to block change simply because of their "comfort level" at the way things are now. Selling the "future state" and change necessity is a high priority item for the entire management team.

6. **Celebrations:** As critical matters become resolved during different times of the transition then ceremonies should be held to celebrate. It not only acknowledges the work of that group but re-enforces the committment from others.

7. **Progress Checkpoints:** Throughout the transition period process needs to be measured. This should resolve delays that may impact others and also serves to announce victories.

CONCLUSIONS, RECOMMENDATIONS AND FUTURE IMPLICATIONS

CONCLUSIONS

The purpose of this study was to examine the feasibility of statewide Law Enforcement Information Systems Networking by the Year 2000. Specific consideration was given to public support, law enforcement willingness to share information with other departments, technological advances, and funding methods.

The trends would indicate a high probability of a statewide system occurring if supported by appropriate planning and management. The research has found that the people of the State of California are very much interested in protecting their "Quality of Life". To this end, law enforcment should enjoy strong public support in the future. This requires, however, a strong police-public partnership. Methods to further develop and maintain this pardnership include community relations programs that focus on law enforcement efforts to resolve criminal problems. Specific to our issue should be the value gained through information systems networking.

Law enforcement agencies are beginning to view the value and necessity of systems networking. National efforts are being made to provide law enforcement with more data being collected at the federal level. We have seen several efforts of networking systems at the county or regional level. If these trends continue, as forecasted, there should be a high level of willingness by law enforcement to join in a statewide network.

Technological advances in hardware, software, and telecommunications will further support a statewide system. "Technology is advancing so rapidly that the field of information management - once clouded in obscurity - has achieved a position of primary importance in just a few decades". (Nemeck, 1990)

It is expected that these trends will continue making a system for our "desired future" more feasible. "Police executives and

agencies of all sizes must keep abreast of this technology if they are to continue to deliver the sophisticated services demanded today". (Cameron, 1990)

This study, has concluded also, that funding will play a major role in getting us from where we are today into the "desired future". Creative efforts at local, state, and in some cases federal levels, must be developed to support our systems networking.

If California Law Enforcement is expected to meet the demands of an increasingly mobile society then a necessary conclusion is that they must do a better and faster job of sharing information with one another.

RECOMMENDATIONS

Law enforcement in the State of California must prepare now, for what might be the most effective crime fighting tool by the year 2000.

We have viewed the future in three possible "scenarios" and it is apparent that the "desired state" will lead to more effective and efficient criminal investigation.

Major social and political issues of California Law Enforcement Information Systems Networking surfaced during this research. Much of the strategic planning, policy development, and the transition management plan focused on these areas. Due to limitations on the length of this study, a more indepth look at technological advances is left to future researchers.

FUTURE IMPLICATIONS

Law enforcement, on the heals of private industry, is realizing that networking is truly the wave of the future. "Despite the risks, businesses are stringing computers together at an

astonishing rate. This year, U.S. companies will hookup 3.8 million personal computers and small office networks, raising the total by 48% over 1989. Many of these networks will tie into mini-computers and main frames that also control thousands of terminals and printers in offices, banks, factories, and supermarkets". (Verity, 1990)

Similar risks and similiar investment will be one of law enforcement's challenges of the 90's. Beyond statewide networking exists the potential for more and improved systems interstate, nationally, and internationally. Only by preparing ourselves for the year 2000, can we lay the foundation for law enforcement in the years beyond.

REFERENCES CITED

1. Jerry Cameron, Artificial Intelligence, Expert Systems, Micro-Computers and Law Enforcement, The Police Chief, March 1990, p. 36.

2. Anita Hipius Shaw, Clearing The Hardware and Software Smoke Screen, Law Enforcement Technology, October 1989, p. 45.

3. David F. Nemecek, NCIC 2000: Technology Adds A New Weapon To Law Enforcement's Arsenol, The Police Chief, April 1990, p. 30.

4. John W. Verity, Peter Coy, Jeffrey Rothferer, Taming The Wild Network, International Business Week, October 8, 1990, p. 67.

BIBLIOGRAPHY

Baker, Richard H. The Computer Security Handbook. Pennsylvania: TAB Professional and Reference Books, 1985.

Bennett, Georgette. Crime Warps - The Future of Crime in America. New York: Anchor Press/Doubleday, 1987.

Capron, H. L., and Williams, Brian K. Computers and Data Processing. 2nd ed. California: Benjamin/Cummings, 1984.

Murdick, Robert G.; Ross, Joel E.; and Claggett, James R. Information Systems For Modern Management. 3rd ed. New Jersey: Prentice-Hall, 1984.

Naisbitt, John. Megatrends - Ten New Directions Transforming Our Lives. New York: Warner Books, 1982.

Orwell, George. 1984. New York: Hancourt Brace Jovanovich, 1949.

Roszak, Theodore. The Cult of Information. New York: Pantheon Books, 1986.

APPENDICES

TRENDS

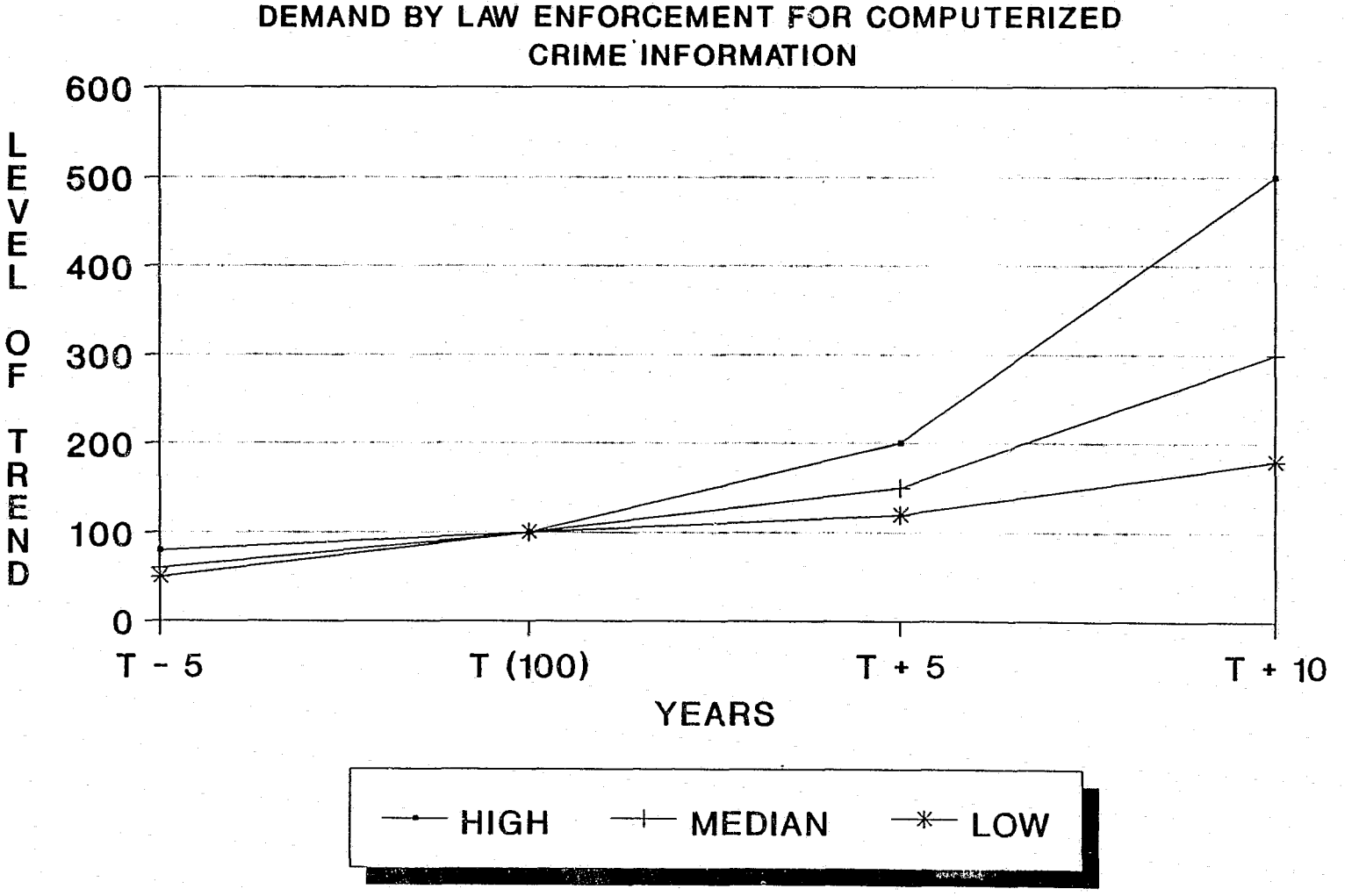
* 1. Demand by law enforcement for computerized crime information. (Number 1)
  2. Increase in population.
  3. Isolation in systems.
  4. Cost of computers coming down.
* 5. Demands by the public to solve crime economically. (Number 4)
  6. Reduction in the size of equipment and it being more mobil.
  7. Increased mobility of society.
  8. Mere emphasis on law enforcement education.
  9. Higher crime rate.
  10. Innovative public financing, private investments in public safety and asset seizures supplementing shrinking tax dollars.
*11. Willingness by the police to learn and use automation. (Number 3)
  12. Computers becoming faster and simpler to use.
  13. Higher sophistication in criminals.
  14. Reliance in private services.
  15. Faster networking technology.
*16. Legal mandates for the collection and sharing of information. (Number 5)
  17. Increase in non-secure custody prisoners.
  18. Rise in concern for network security.
  19. More use of civil process.
  20. Past commitment vs. future cost - Re-tooling
  21. Willingness by the general public to support data banks to control crime. (Number 2)
  22. Growing public impatience.
  23. More and better information being collected and available.
  24. Separation of state, county, and city.

25. More consolidation of services.
26. Regionalization for dealing with crime issues.
27. Now and improved methods of personal identification.
28. Community partnership.
29. Reduction in transportation available to law enforcement.
30. Awareness of need to network.
31. Media setting law enforcement agenda.
32. Punishment oriented society.
33. Flexibility - changing social values.
34. Other non-traditional law enforcement having need for information also.
35. Fixed enforcement.

EVENTS

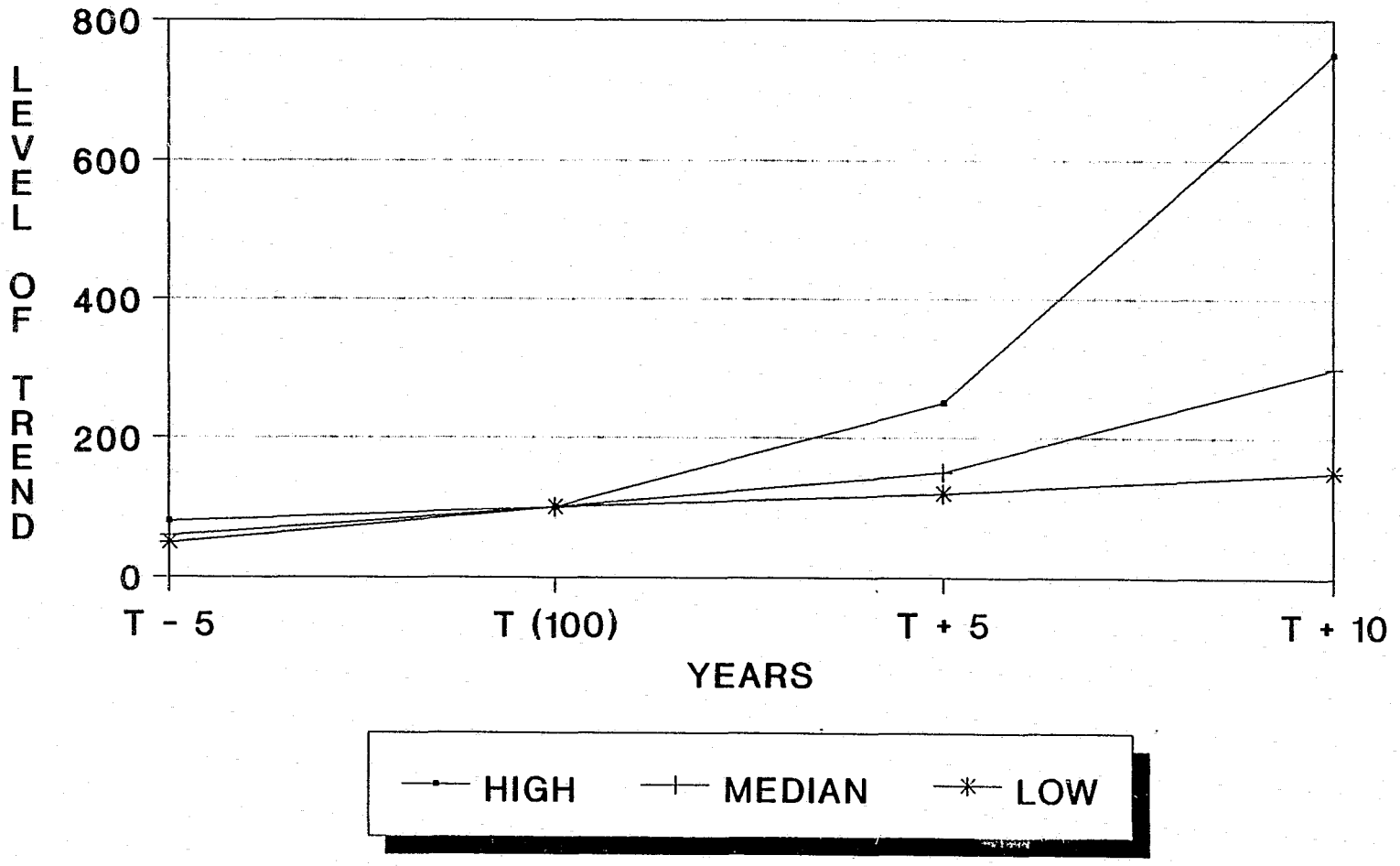
1. Technological breakthrough occurs to link different hardware together.
2. Major natural or manmade disaster occurs.
3. Robotics replace Human Resources.
4. State and Federal funding assists local government in computer purchases for law enforcement.
5. State mandates automated uniformed crime reports.
6. The private sector contracts for data processing - new business.
7. State or National Police Force replaces city and county law enforcement agencies.
8. Collapse of local government in ten cities.
9. Combining of city and county governments.
10. State mandates individual identification and we have instant personal identification methods.
11. Prop. 2013 - Mandatory cost reduction.
12. Paperless Police Department.
13. Court policy changes to allow the public collection of all data mandated public access to data.
14. Major economics decline.
15. Geographic realignment.
16. IBM donates regional computer system.
17. Voice recognition system is fully developed.
18. Legalization of drugs.
19. Visual communications systems are fully developed.
20. Computer terminals are on every desk and in every police vehicle.
21. New source of energy is found.
22. Computer knowledge becomes a job requirement in law enforcement.
23. Artificial intelligence is developed.

TREND ONE EVALUATION
NOMINAL FORECAST



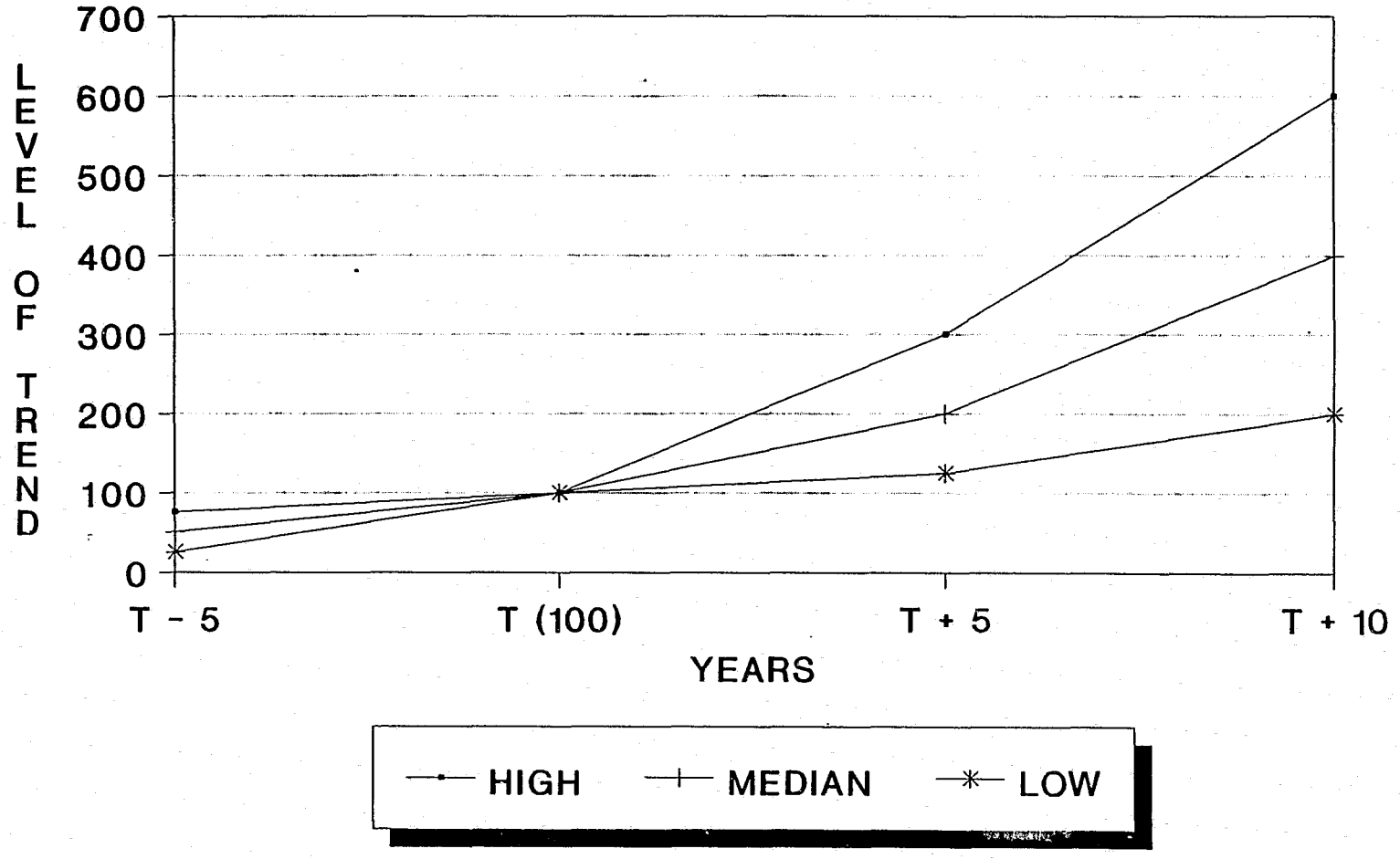
TREND TWO EVALUATION
NOMINAL FORECAST

THE LEVEL OF WILLINGNESS BY THE GENERAL PUBLIC TO SUPPORT DATA BANKS TO CONTROL CRIME



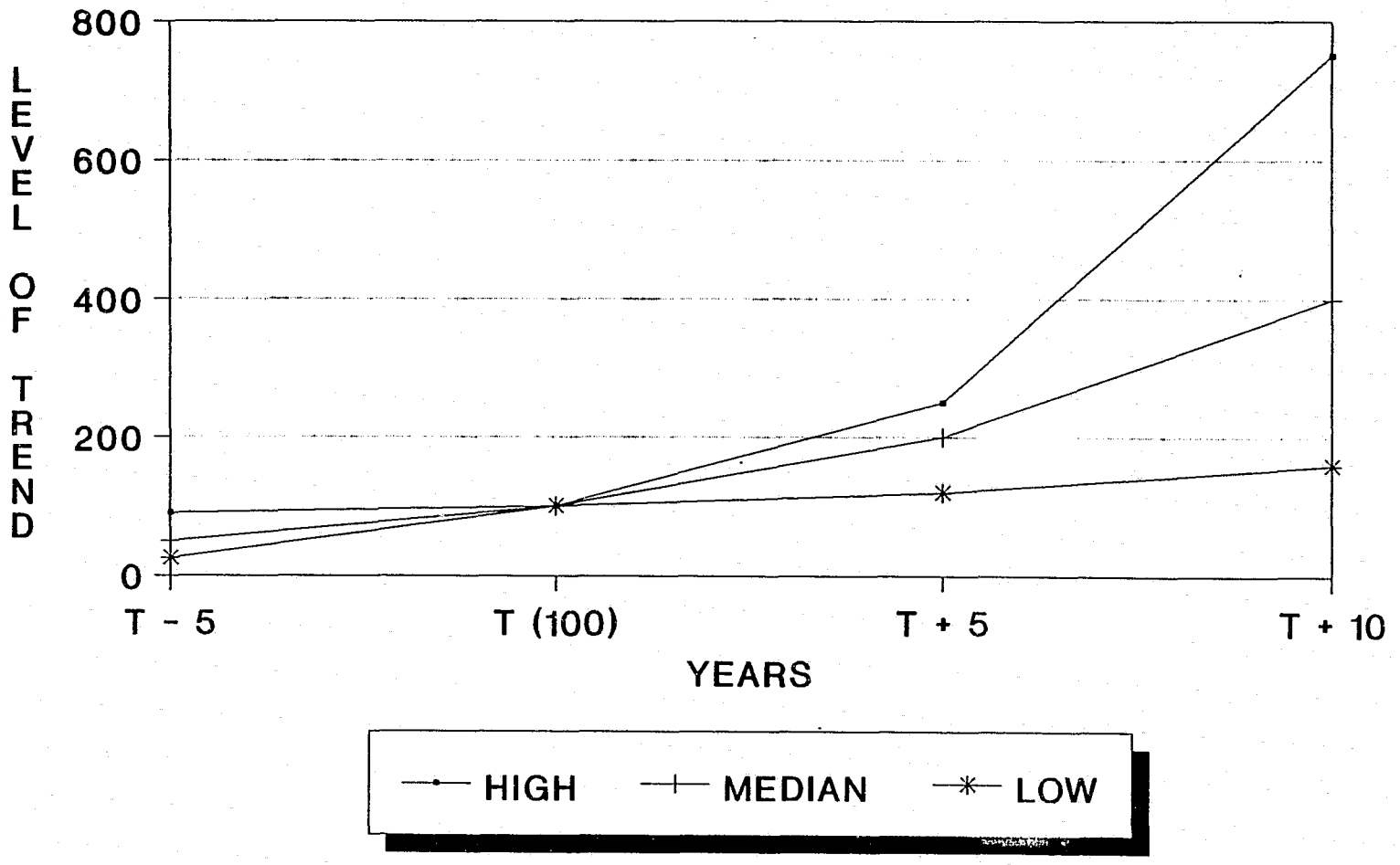
TREND THREE EVALUATION
NOMINAL FORECAST

WILLINGNESS BY THE POLICE TO LEARN AND USE INFORMATION



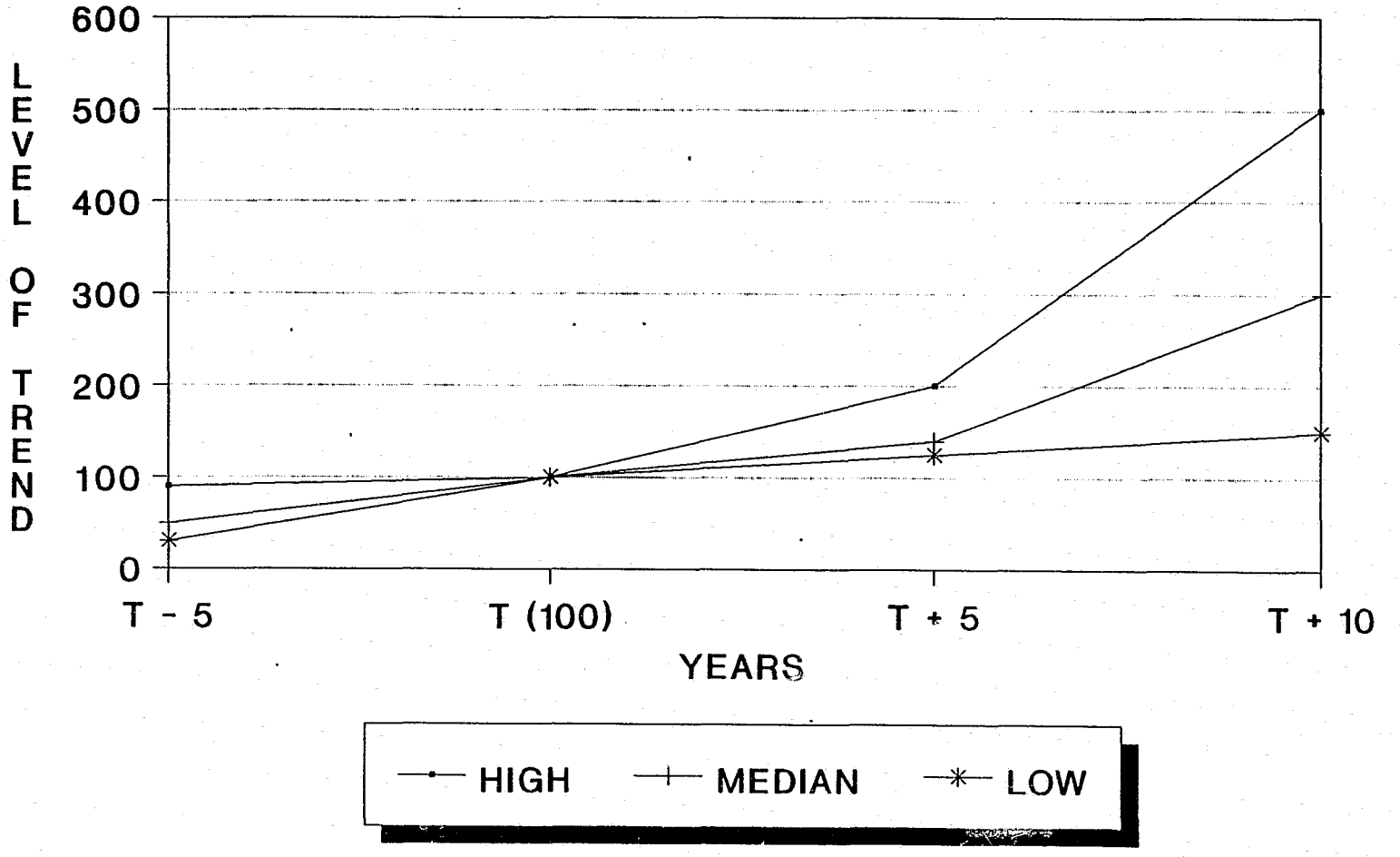
TREND FOUR EVALUATION
NOMINAL FORECAST

DEMANDS BY THE PUBLIC TO SOLVE CRIMES ECONOMICALLY



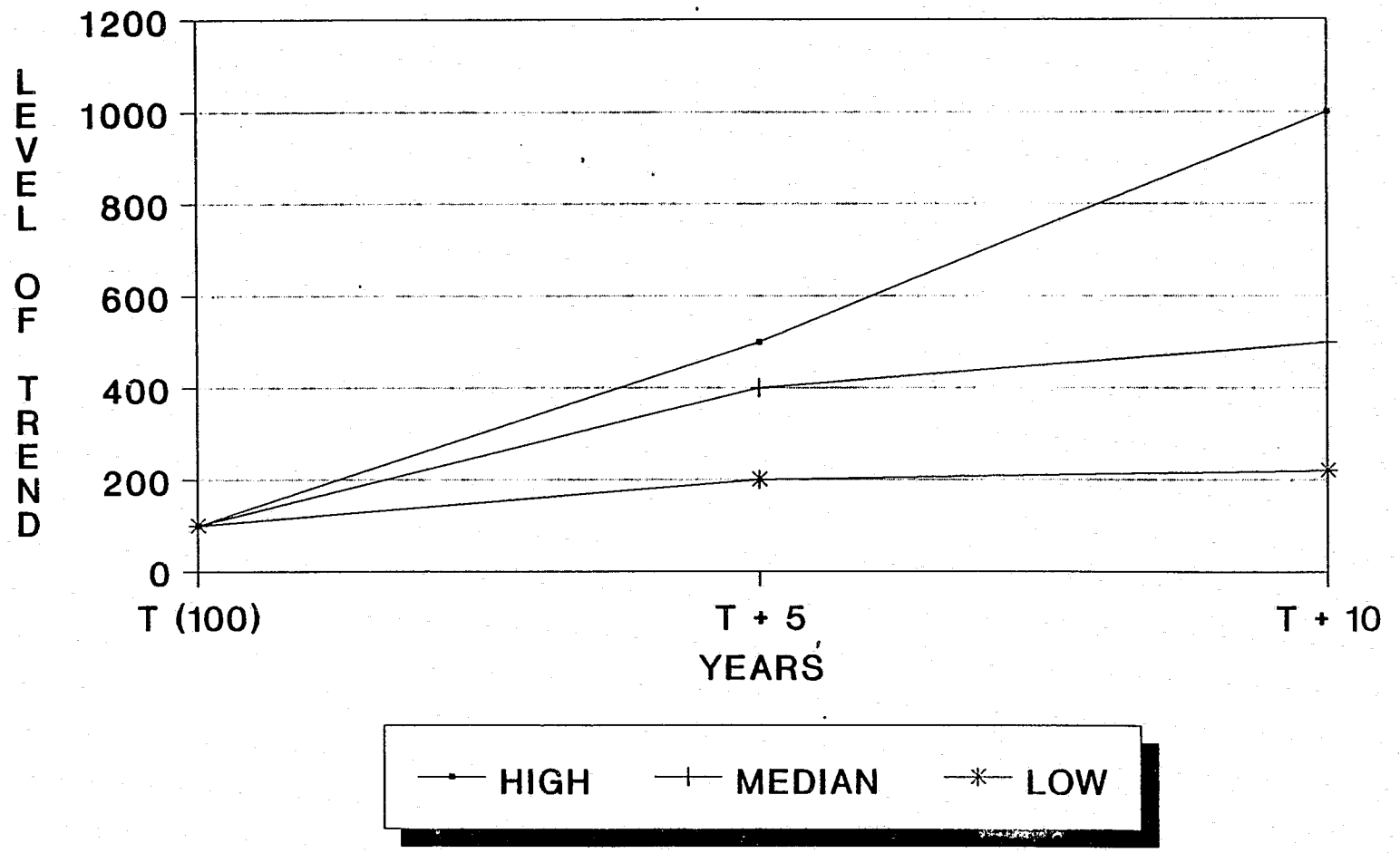
TREND FIVE EVALUATION
NOMINAL FORECAST

LEGAL MANDATES FOR THE COLLECTION AND SHARING OF INFORMATION



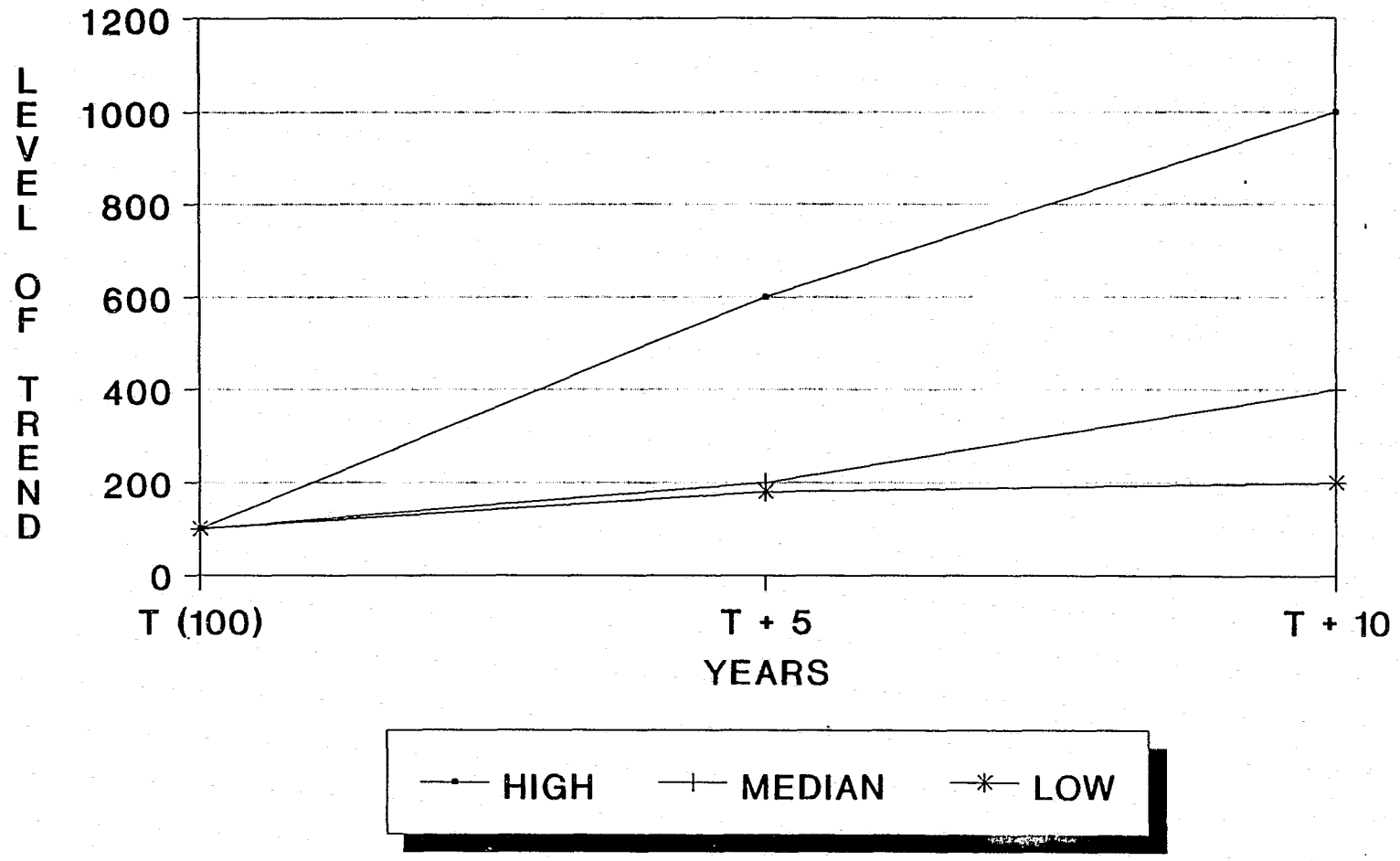
TREND ONE EVALUATION
NORMATIVE FORECAST

DEMAND BY LAW ENFORCEMENT FOR COMPUTERIZED CRIME INFORMATION



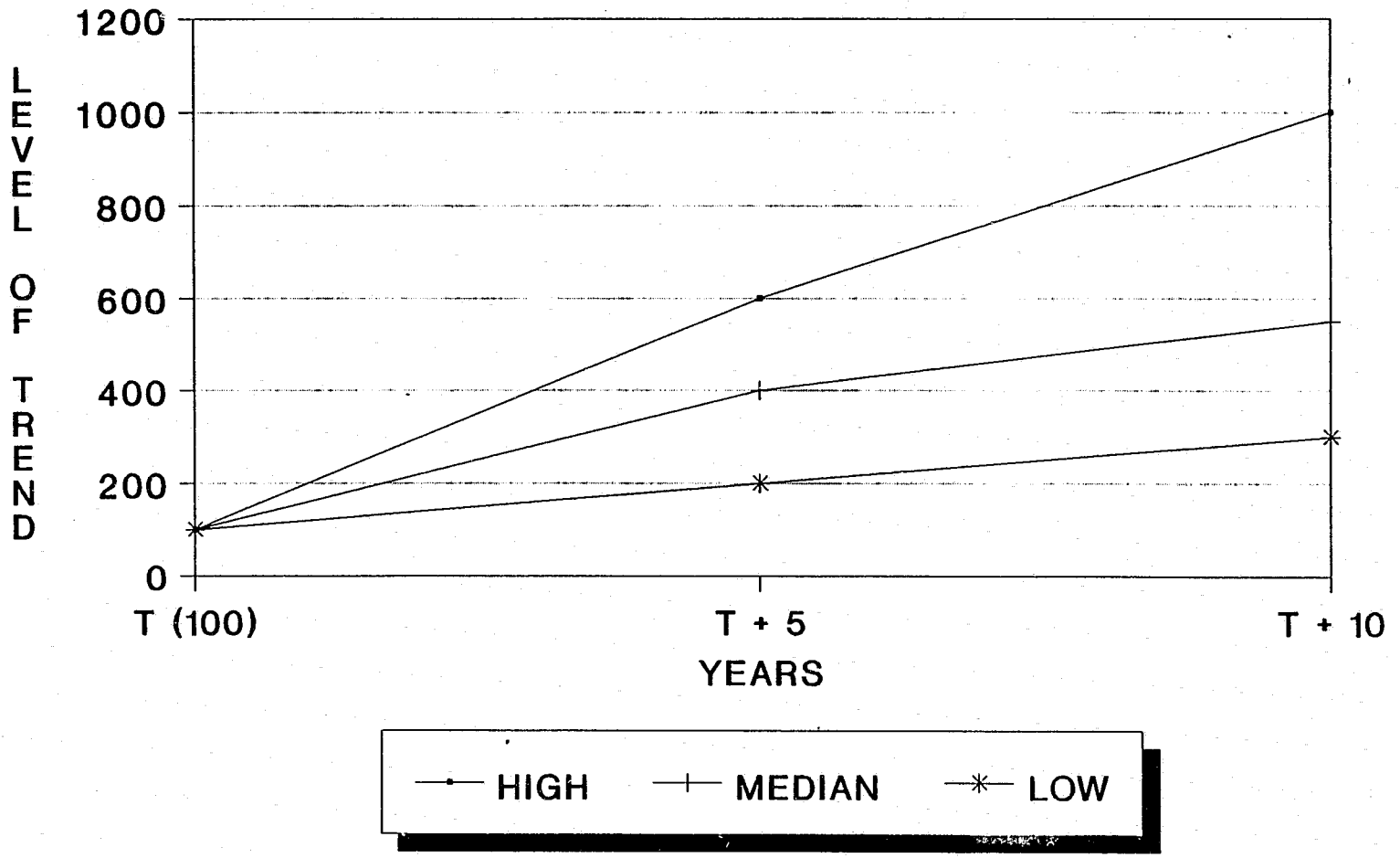
TREND TWO EVALUATION
NORMATIVE FORECAST

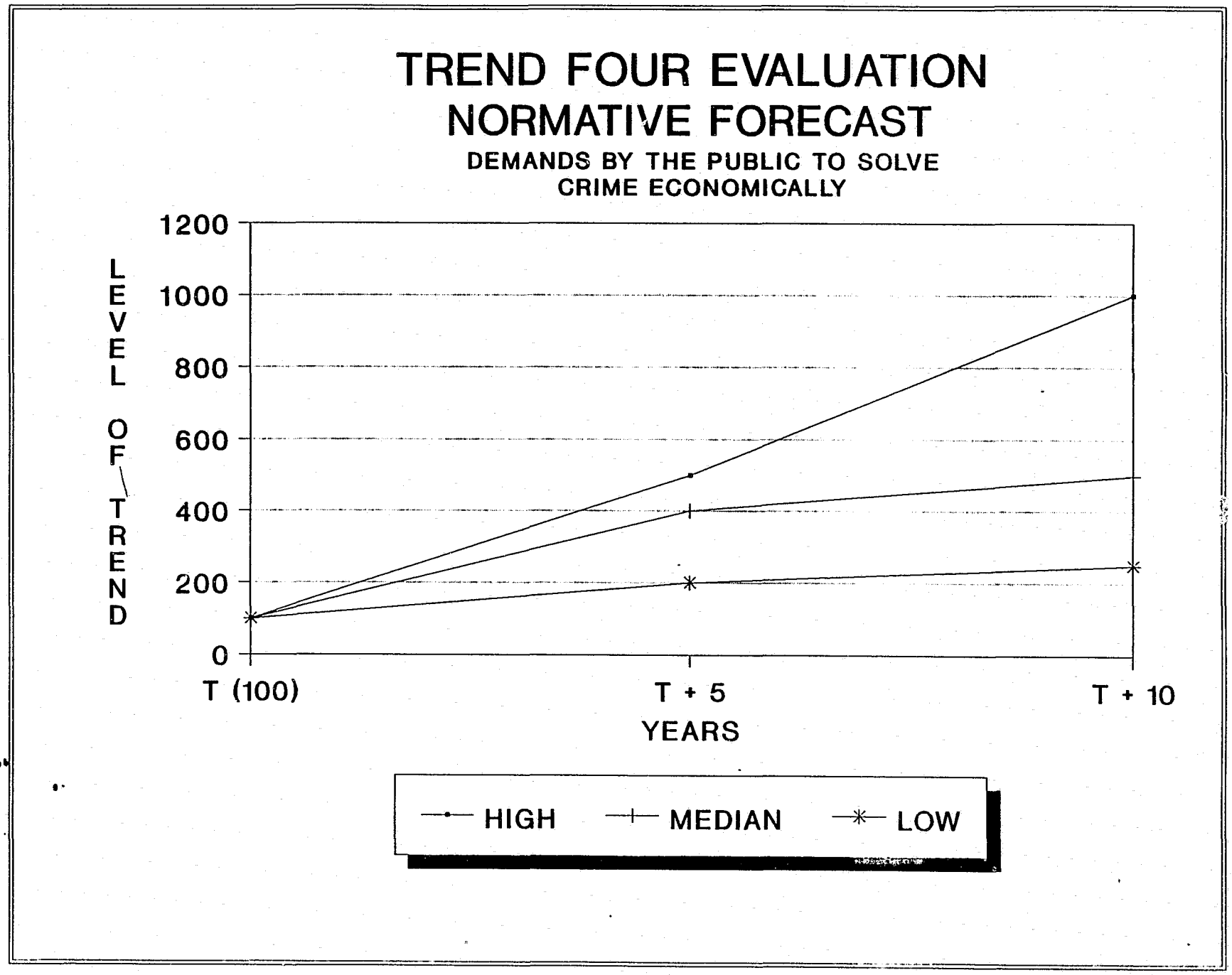
THE LEVEL OF WILLINGNESS BY THE GENERAL PUBLIC TO SUPPORT DATA BANKS TO CONTROL CRIME



TREND THREE EVALUATION
NORMATIVE FORECAST

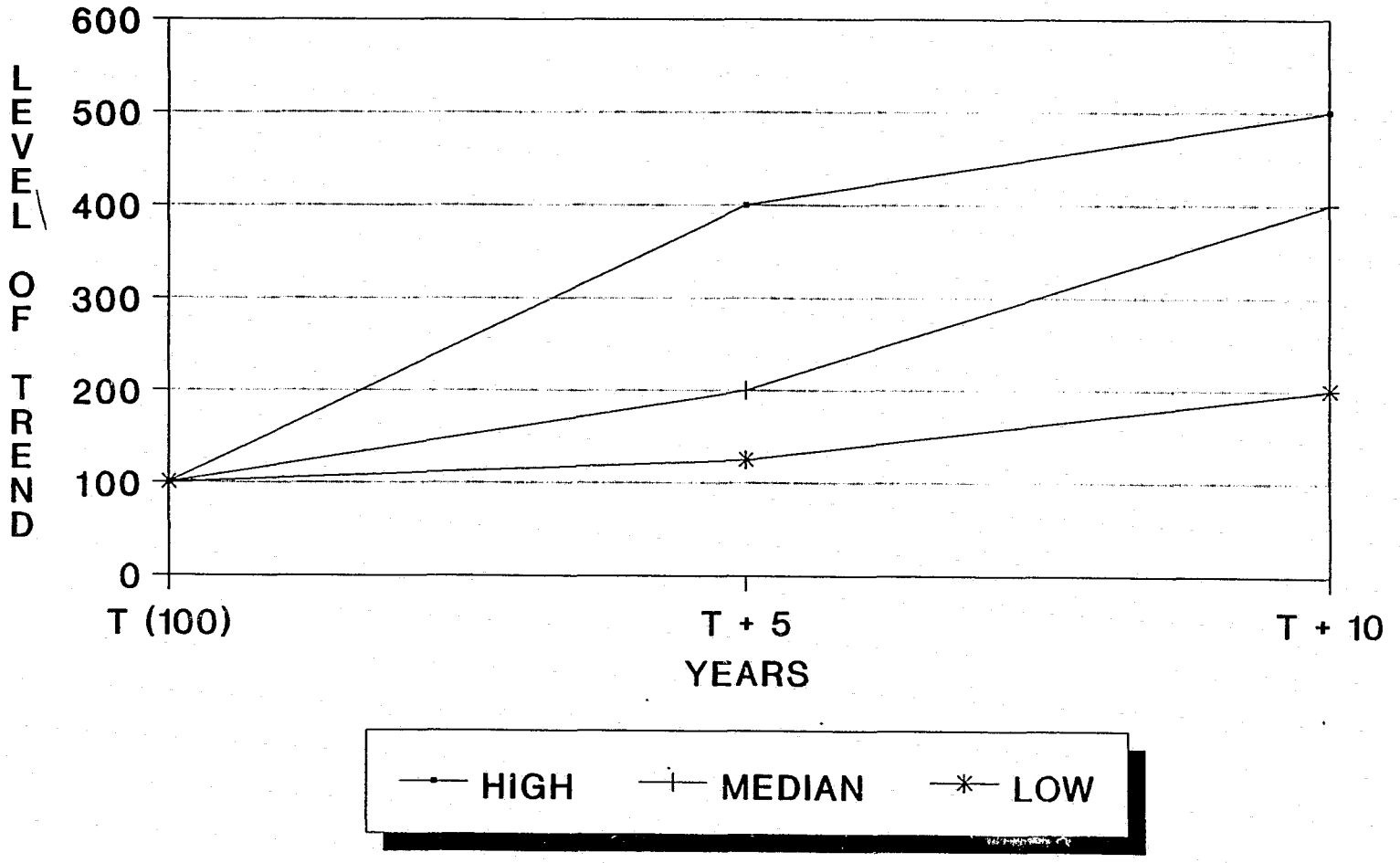
WILLINGNESS BY THE POLICE TO LEARN AND USE INFORMATION



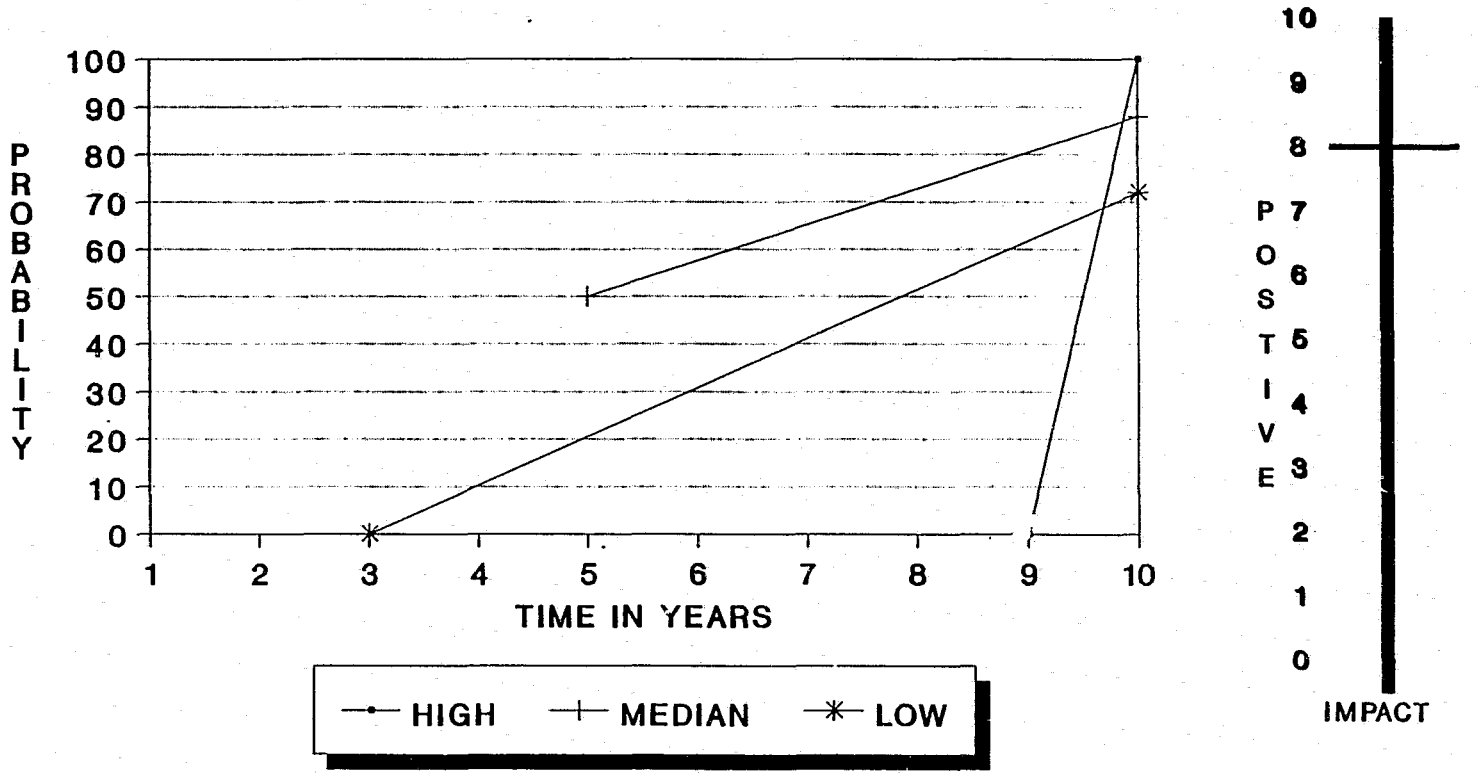

TREND FOUR EVALUATION
NORMATIVE FORECAST
DEMANDS BY THE PUBLIC TO SOLVE
CRIME ECONOMICALLY
LEVEL OF TREND
1200
1000
800
600
400
200
0
T (100)
T + 5
T + 10
YEARS
HIGH
MEDIAN
LOW

TREND FIVE EVALUATION
NORMATIVE FORECAST

LEGAL MANDATES FOR THE COLLECTION AND SHARING OF INFORMATION

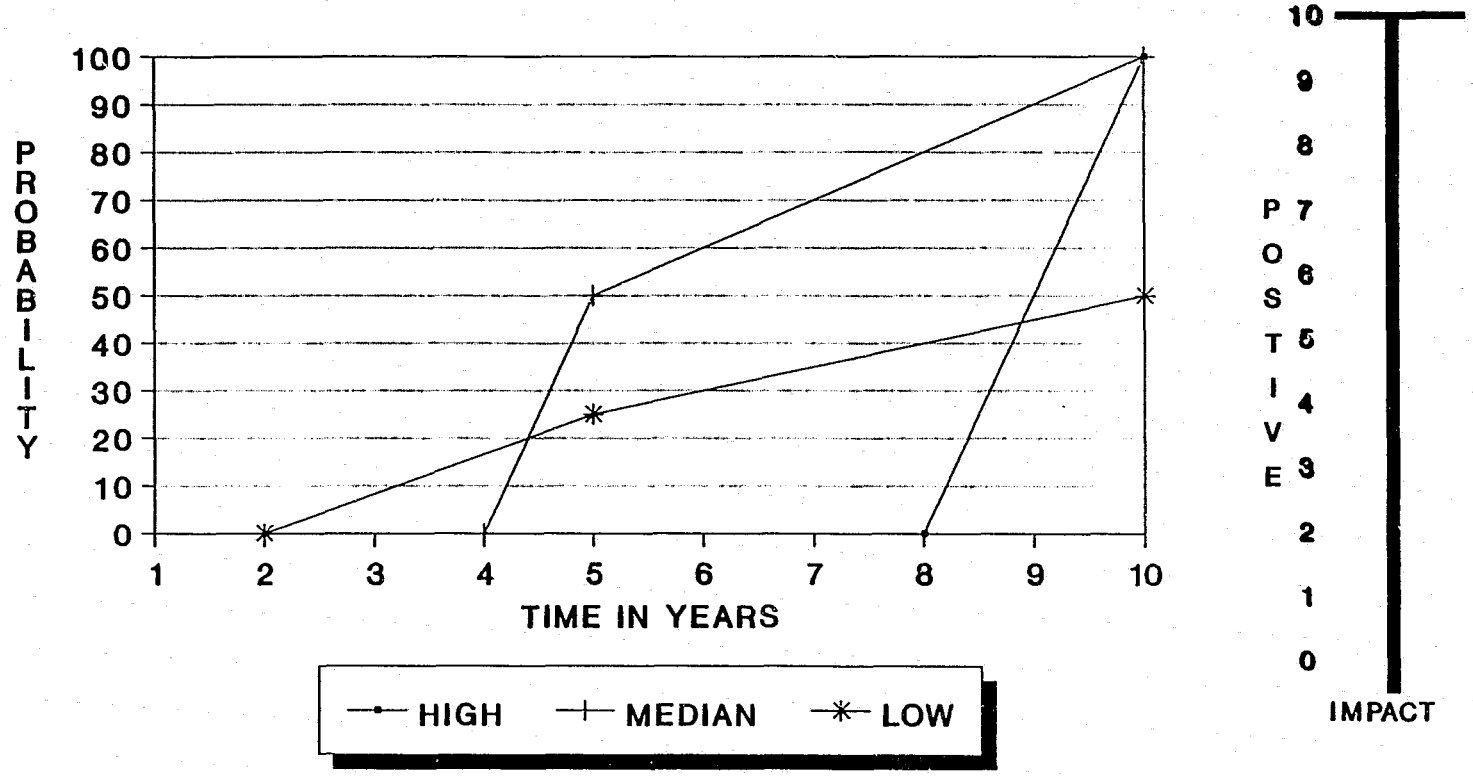


EVENT ONE
EVALUATION GRAPH



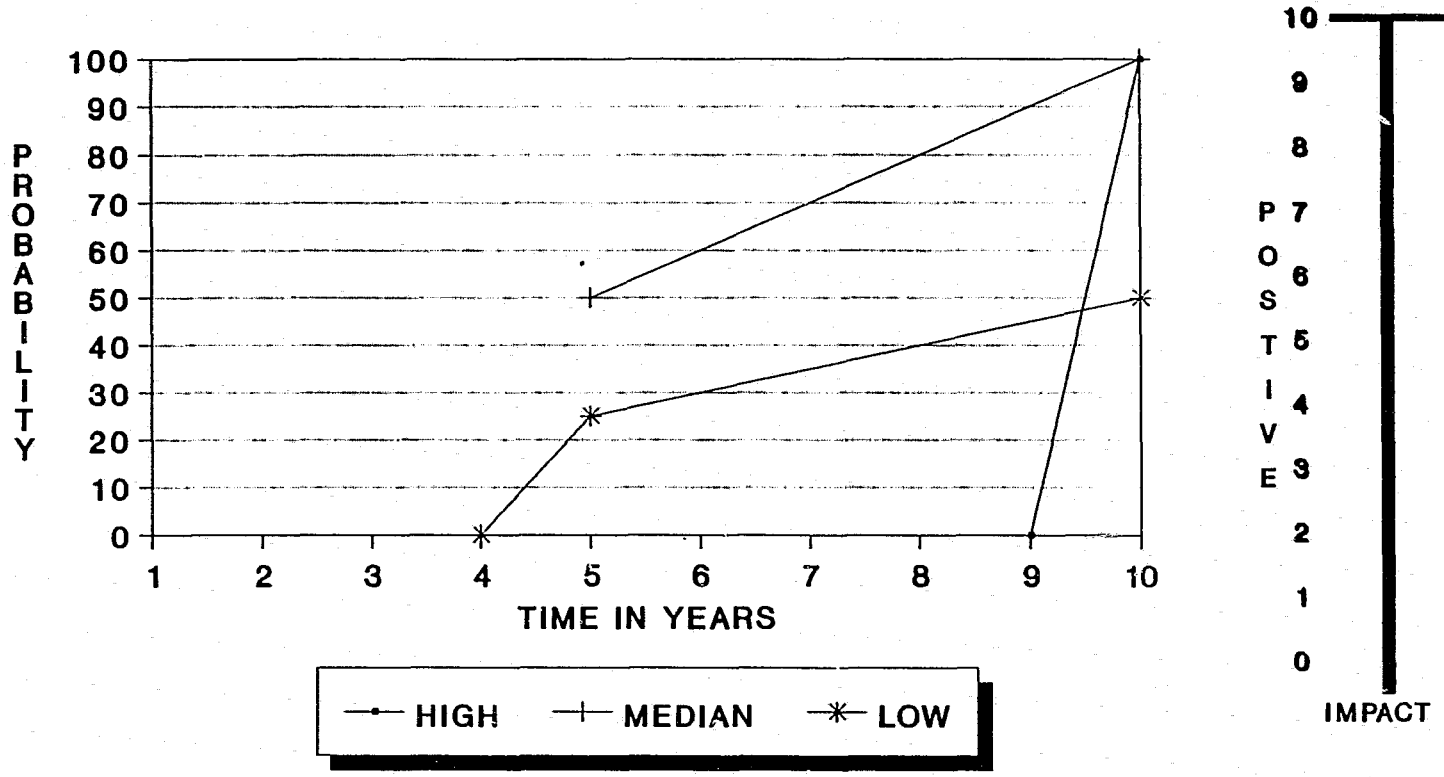
COMPUTER TERMINALS ARE ON EVERY DESK AND
IN EVERY POLICE VEHICLE

EVENT TWO
EVALUATION GRAPH



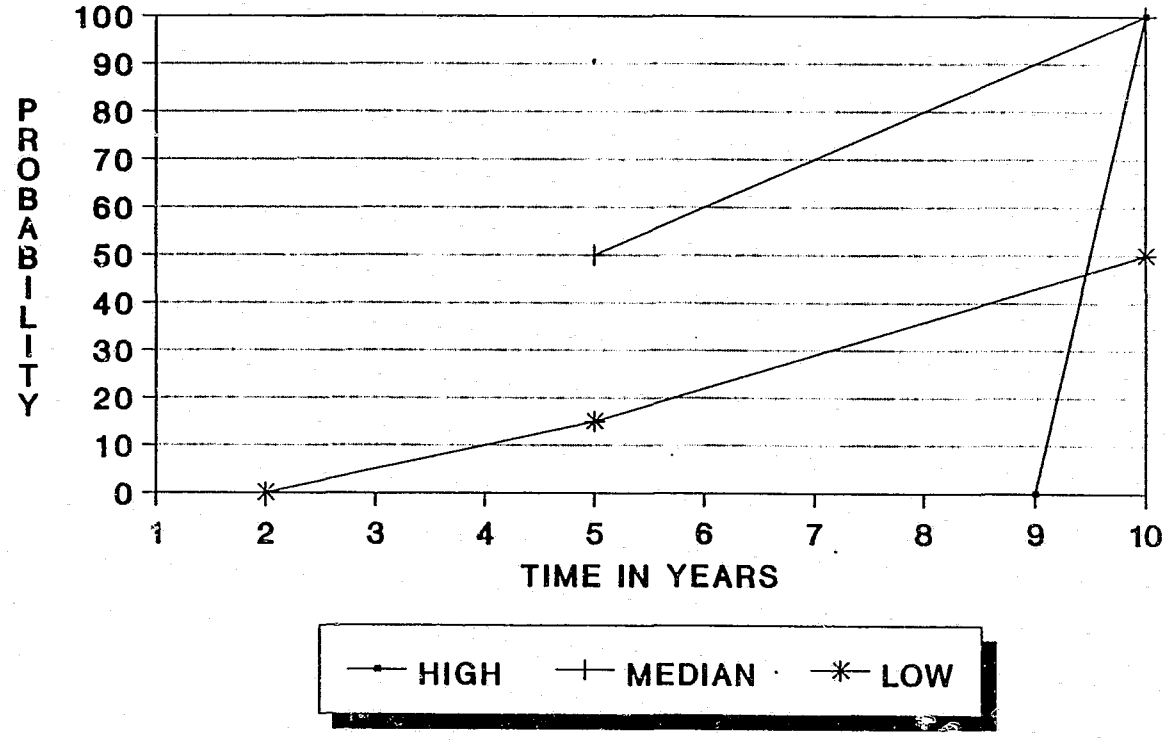
A TECHNOLOGICAL BREAKTHROUGH OCCURS TO LINK DIFFERENT HARDWARE SYSTEMS TOGETHER

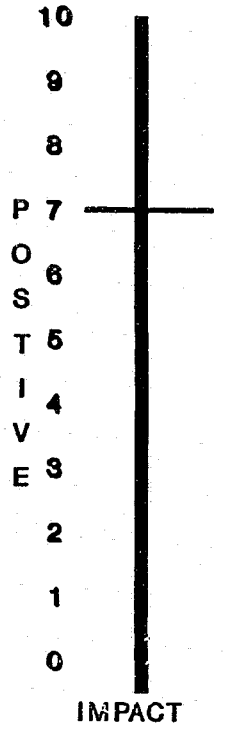
EVENT THREE
EVALUATION GRAPH



THE STATE DEPARTMENT OF JUSTICE DEVELOPS A PROGRAM TO PAY FOR 75% OF LOCAL POLICE COMPUTER SYSTEMS

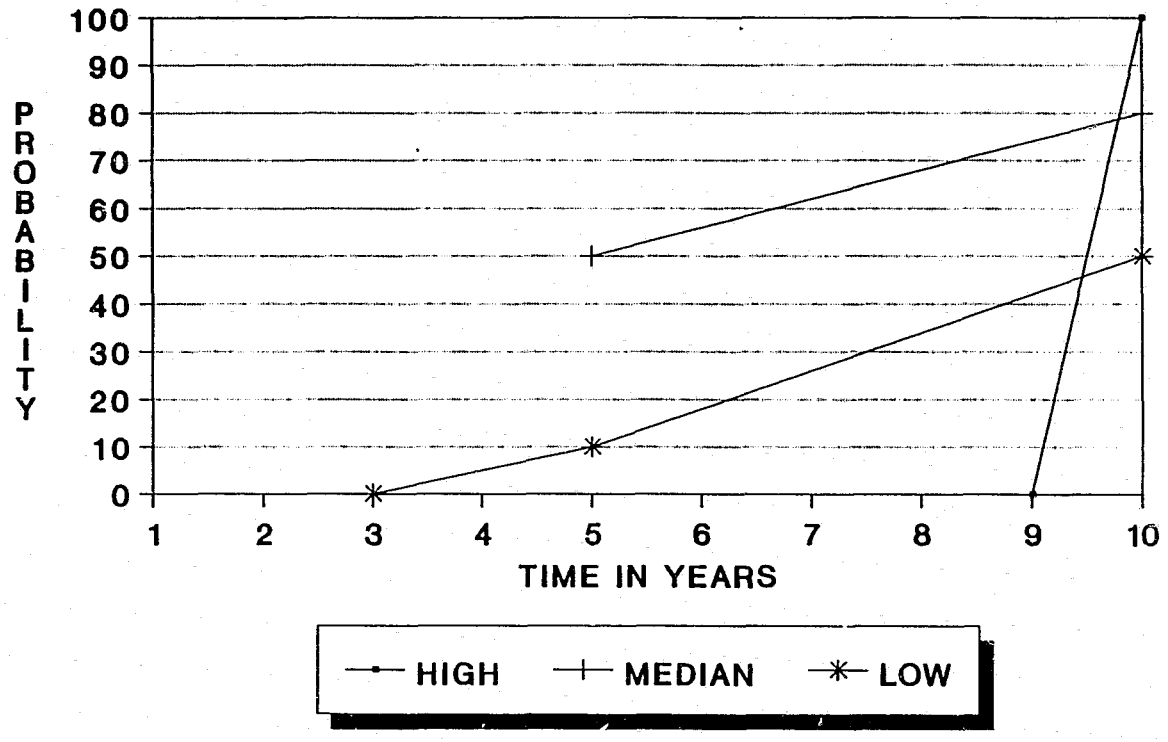
EVENT FOUR
EVALUATION GRAPH

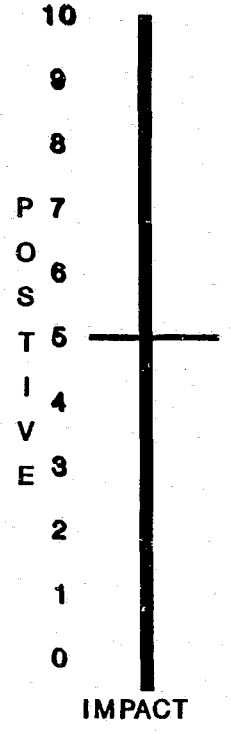




THE STATE MANDATES AUTOMATED UNIFORMED CRIME REPORTS

EVENT FIVE
EVALUATION GRAPH





ALL DEPARTMENTS BECOME PAPERLESS

Trend #	TREND STATEMENT (Abbreviated)	LEVEL OF THE TREND ** (Today = 100)			
		5 Years Ago	Today	* Five years from now	* Ten years from now
T-1	Demand by law enforcement for computerized crime information.	60	100	150 400	180 500
T-2	Willingness by the general public to support data banks to control crime.	60	100	150 200	300 400
T-3	Willingness by the police to learn and use automation.	50	100	200 400	400 550
T-4	Demands by the public to solve crimes economically.	50	100	200 400	400 500
T-5	Legal mandates for the collection and sharing of information.	50	100	140 200	300 400
			100		
			100		
			100		
			100		
			100		

** Panel Medians

* Five years from now
"will be" / "should be"

* Ten years from now
"will be" / "should be"

Event #	EVENT STATEMENT	* YEARS UNTIL PROBABILITY FIRST EXCEEDS ZERO	* PROBABILITY		IMPACT ON THE ISSUE AREA IF THE EVENT OCCURRED	
			Five Years From Now (0-100 %)	Ten Years From Now (0-100%)	* POSITIVE (0-10 scale)	* NEGATIVE (0-10 scale)
E-1	Computer terminals are on every desk and in every police car.	5	50%	90%	8	0
E-2	A technological breakthrough occurs to link different hardware systems together.	4	50%	100%	10	0
E-3	The State Department of Justice develops a program to pay for 75% of local police computers.	5	50%	80%	10	0
E-4	State mandates automated uniform police reports.	5	50%	100%	7	0
E-5	All police departments become paperless.	5	50%	80%	5	0

* Panel Medians

BASIC CROSS-IMPACT EVALUATION MATRIX

IMPACTING EVENT (ACTORS)	IMPACTED EVENT (REACTORS)					IMPACTED TRENDS (REACTORS)					IMPACT
	E-1	E-2	E-3	E-4	E-5	T-1	T-2	T-3	T-4	T-5	Event Impacts
E-1 Computer terminals are on every desk and in every police car. * 90	X	0	0	15	100	100	85	100	90	0	6
E-2 A technological breakthrough occurs to link different hardware systems together. *100	25	X	50	100	50	100	100	100	80	50	0
E-3 The State Dept.of Just. develops a program to pay for 75% of local police computers. * 80	100	0	X	75	30	100	85	100	90	100	8
E-4 State mandates automated uniform police reports. *100	0	0	0	X	50	70	50	90	0	90	5
E-5 All police departments become paperless. * 80	100	0	20	0	X	100	50	100	50	25	7
EVENT AND TREND REACTORS (IMPACTS OR "HITS")	3	0	2	3	4						

*PROBABILITY OF EVENT OCCURRING.

Events on Events
Percentage change (+ or -)

Events on Trends
Percentage change (+ or -)

RESPONSIBILITY CHART

R= Responsibility (not necessarily authority)
A= Approval (right to veto)
S= Support(put resources toward)
I= Inform (to be consulted)
- = Irrelevant to this item

Actors

Decision/Task		PROJECT MANAGER	LAW ENFOR. MANAGERS	INVESTI-GATORS	INFO SYSTMS MANAGERS	CHIEFS / SHERIFFS	TECHNICAL SUPPORT	LEGISLATIVE ADVISORS	CITIZENS GROUP										
EVALUATE EXISTING SYSTEMS		I	S	S	R	S	S	-	-										
WORK WITH VENDORS TO DEVELOP THE NETWORK SYSTEM		A	A	A	A	A	R	S	I										
IDENTIFY DIFFERENT METHODS OF FUNDING		A	I	-	I	R	-	A	I										
WORK TO GAIN AND MAINTAIN PUBLIC SUPPORT		I	A	I	A	R	-	A	A										
WORK WITH POST TO IDENTIFY AND PLAN TRAINING.		A	R	I	S	S	I	I	I										
RECRUIT PERSONNEL		I	I	I	R	A	A	I	I										
OBTAIN SUPPORT FROM CHIEFS AND SHERIFFS		S	S	-	S	R	-	S	I										
DEVELOP REPORTS FOR INVESTIGATORS		A	A	R	A	A	S	I	I										