

**HOW WILL BIOMETRIC TECHNOLOGY IMPACT SITE SECURITY IN A
SMALL UNIVERSITY POLICE DEPARTMENT BY 2009?**

**A project presented to
California Commission on
Peace Officers Standards and Training**

By

**Chief Fred D. Hardee, Jr.
California State University Monterey Bay Police Department**

Command College Class XXXVI

Sacramento, California

September 2004

This Command College Project is a FUTURES study of a specific 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 view 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).

Copyright 2004

California Commission on Peace Officer Standards and Training

TABLE OF CONTENTS

	LIST OF TABLES AND FIGURES	iii
Chapter I	ISSUE DEVELOPMENT AND LITERATURE SEARCH	1
	The Current State of Biometric Technology	4
	Application of Biometric Technology at CSUMB	7
Chapter II	FORECASTING THE FUTURE	10
	Utilization of the Nominal Group Technique	10
	Strategic Purpose and Definitions	11
	Trend Summary	12
	Event Summary	19
	Cross Impact Analysis	25
	Futures Scenarios	28
	Pessimistic Scenario	28
	Optimistic Scenario	29
	Surprise Free Scenario	30
	Why Look Ahead?	31
Chapter III	STRATEGIC PLANNING.....	33
	Strategic Planning	33
	Organization Analysis – Strengths and Weaknesses.....	35
	Stakeholder Identification and Analysis.....	37
	Development of Alternative Strategies	40
	Selection of the Appropriate Strategy.....	41
Chapter IV	TRANSITION MANAGEMENT	43
	Transition Planning.....	43
	Assess Organization / Stakeholder Readiness	44
	Establish Steering Committees	44
	Develop a Shared Vision	44
	Foster Consensus	45
	Share the Vision	45
	Financial Resources Required for implementation.....	46
	Policies Required for Implementation.....	47
	Transition Management and Critical Mass.....	47
	Commitment Planning: Critical Mass Evaluation.....	47
	Critical Mass Commitment.....	48
	Transition Management Structure	49
	Techniques and Methods of Implementation.....	50
	Responsibility Charting.....	51

Chapter VI	RECOMMENDATIONS AND CONCLUSIONS	54
	Recommendations	55
	The Leadership Factor	53
	Conclusions.....	56
	 APPENDICES	
	Nominal Group Technique Panel (NGT) Members	59
	Potential Trends Identified by NGT Panel	60
	Potential Events Identified by NGT Panel	61
	 ENDNOTES.....	62
	 BIBLIOGRAPHY	64

LIST OF TABLES AND FIGURES

Table 2.1	Strategic Purpose Statement	12
Table 2.2	Definitions	12
Table 2.3	Trend Summary Table	13
Table 2.4	Event Summary Table.....	19
Table 2.5	Cross Impact Table	26
Table 4.1	Critical Mass Commitment Chart.....	49
Table 4.2	Responsibility Chart	52

CHAPTER 1

ISSUE DEVELOPMENT

Issue Definition

This project focuses on the following question: How will biometric technology impact site security in a small university police department by 2009? Biometric technology refers to the automated capture of a person's unique biological data that distinguishes him or her from another individual. Biometrics can be measured in many forms, including fingerprints, voice patterns, iris patterns, hand geometry and facial features. The main reason biometrics works for identification is that individuals cannot control these unique aspects of their biology; for example, a person cannot change their fingerprint or the identifying features of their iris.¹

The state of California Commission on Peace Officer Standards and Training (POST) defines a small California law enforcement agency as a law enforcement organization of 49 or fewer personnel. A mid-size agency is 50 to 499 sworn officers and a large agency is over 500 sworn officers.² Although the focus of this project emphasizes a small-size university law enforcement agency's implementation of biometric technology as it relates to site security, the strategies have implications for university or college law enforcement agencies of all sizes.

Introduction

In a basic sense, there are two phases involved in implementing biometrics. The first phase involves having an individual's physiological characteristics recorded. This can be accomplished by having a fingerprint, iris, hand or face scanned. The data from

the scan is converted to a unique template, encrypted, and stored as numerical data. The second phase requires the individual to present his or her unique features (fingerprint, iris, hand, or face) for comparison with the data previously recorded. The system then returns a “yes” or “no” after comparing the presented data with data already on file.³

Biometrics can be used in two ways – verification and identification. Verification is the act of authenticating an individual’s identity by comparing the biometric data to the data previously on file.⁴ This is considered a one-to-one search because it is comparing the information an individual is presenting to the information already on file for the particular individual. In this particular case, there is not a search of an entire database for the unique biometric feature, but rather a verification that authenticates the individual is who he or she claims to be.

Identification is similar in concept to verification, except the presented biometric data is compared to the entire population enrolled in the system via a search of the entire database. This is sometimes referred to as a “one-to-many” search technique because an entire database is searched to match the presented biometric data with that information already in the database.⁵

Biometric verification and identification leads to one of three outcomes: a positive match, a false rejection, or a false acceptance. A positive match indicates the person is who he/she says they are. A false rejection occurs when an authorized user is rejected and a false acceptance occurs when an imposter is accepted as an authorized user.⁶

There are a variety of biometric technologies currently available. Some are more popular and more technologically advanced than others, with the fingerprint being the most common. Other biometric technologies include the iris scan, hand geometry, facial

recognition, facial thermography and voice recognition.⁷ The technologies are further described as follows:

Iris Scanning Devices: The iris scan operates by using a photograph of an individual's iris. If the iris data matches what is on file, the individual is granted access to the desired event or site. The iris scanner can read through contact lenses, glasses, and most sunglasses. Researchers say the iris is the most unique feature of the human body with 266 measurable characteristics (as opposed to approximately 35 in fingerprints) and does not change over time. They also claim iris scanning is more accurate than DNA testing.

Hand Geometry Devices: Hand geometry is based on the shape of the hand. A device measures finger length, thickness, and curvature. It is used for authentication rather than identification. The data is easier to collect because there isn't a need for good skin contact like is required to obtain a good fingerprint or the need for special lighting required for retina and iris scans.

Facial Recognition: facial recognition is based on capturing facial images by measuring the curves of the face from various angles and measuring the distance between the features. The image is stored as a mathematical algorithm and can be referenced at a later time to verify someone's identity. Facial thermography is implemented by measuring the heat pattern in a person's face. Manufacturers of facial thermography systems claim the systems can identify individuals despite surgery or facial hair. One major drawback of this technology is that alcohol consumption has a drastic effect on the accuracy of thermography.

Voice Recognition: Voice recognition operates by translating voice tones into a

unique corresponding mathematical pattern. A microphone, sound card, and software are required for implementation.

The Current State of Biometric Technology

Biometrics are used in a variety of ways in the United States. One major use of biometrics is for access to sensitive military agencies, intelligence agencies, and other federal organizations requiring very high levels of security. They are also used for physical access control.⁸

Employee time clocks have even moved into the age of biometrics. A time clock company in Florida that has been selling time clocks and punch cards for 30 years is now manufacturing time clocks with fingerprint reading devices. The devices are called the HandPunch system and essentially they work like this: An employee places a hand in the machine and the device photographs the hand three times, noting its dimensions, such as the length and width of the fingers. Then, every time an employee clocks in or out, he or she places a hand on the reader and the device matches the hand size and shape to the image in its memory.⁹ The time is then recorded electronically in the company's computer system, eliminating the need for paper time cards.

At this time, hand readers still have some kinks. Dick Parker, who owns Tampa, Florida-based Edwards Time Equipment, hasn't sold any hand readers yet, but has seen them in action. Parker said the new system takes slightly longer than the old punch card systems. Also, if an employee doesn't place his/her hand on the device properly, it can hang up the process. If a hundred people are waiting to clock in, there will be a wait. "The biometric systems will be the systems of the future," Parker said. "No one has taken it right now and ran with it that much, but eventually, it will be the system."¹⁰

Rex Healthcare of North Carolina recently installed 39 HandKey terminals to heighten security for patients and 3,500 employees at its 61-acre main hospital campus. According to Chris Main, Rex Healthcare Director of Protector Services, “We wanted a higher level of security than a badging system or PIN code alone could offer. After much research, we tested and then chose the biometric HandReaders. We started using the HandKey readers where there was a perceived need for a higher level of security in the birth center. The hand scanners are very accurate. No unauthorized person has ever gotten past one.”¹¹ The HandKey hand readers automatically take a three-dimensional reading of the size and shape of a person’s hand and identify their identity in less than one second. At the hospital, users enter a PIN code that they select and then place their hand on the reader. The system quickly verifies if the hand presented matches the one associated with the PIN, and if so, permits access. HandKey terminals are now used in the birth center, information technology data center, other major information technology areas, the operating rooms and the emergency room department.

When examining the issue of biometric technology and comparing it to the STEEP model¹² (Social, Technological, Economic, Environmental and Political implications), two main obstacles emerge that work against implementation of biometric technology in public facilities; first, the social and political opposition with concerns of violations of the Fourth Amendment, unreasonable search and seizure, the “Big Brother is Watching” fear, as well as worries personal data will be used for something other than its advertised purpose. Despite the formation of a few advocacy groups, mainly sponsored by biometric device manufacturers, there is still no enforceable guidance concerning the use of biometric devices and data.

Regarding the potential social and political opposition to this technology, many feel that privacy is a personal right.¹³ Most individuals desire the ability to maintain some control over their own personal space and to be free of interference from other individuals and organizations. An individual's personal space comes in many forms, including the physical body, personal behavior traits, communication patterns, and personal information. In today's high technology and information age, it is not difficult to collect data about an individual and to use that information to exercise control over the individual. Individuals generally do not want others to have personal information about them unless they decide to reveal it, and individuals are even more leery of third parties who may acquire information without the consent of the rightful owner.

Privacy must be balanced with many competing interests, including the rights of individuals and society as a whole.¹⁴ With the rapid development of technology, it is becoming increasingly difficult to maintain the levels of privacy that citizens knew in the past. Data is being collected everywhere. With advances in databases, datamining, and telecommunications, it is almost effortless to circulate personal information to any interested party.¹⁵

For those advocating the widespread use of biometrics, there appears to be numerous advantages to doing so. Biometric supporters say this technology increases privacy rather than invading it. Many see biometrics as a quality of life enhancement for society as a whole.¹⁶ Some feel biometrics would be a big asset when conducting background investigations to ensure the individual does not have a negative history, particularly in the areas of child abuse and sex offenders.

State welfare programs also fall into the category where biometrics proponents feel the benefits of widespread biometric implementation outweigh personal privacy concerns. In San Diego County, a biometric fingerprint identification system was installed for all welfare recipients. Within the first 18 months of installation, the county paid out \$200,000 less than it normally paid out. The department of social services believes the savings is mainly a result of those who were applying (and receiving funds) for welfare under more than one name.¹⁷

Application of Biometric Technology at California State University, Monterey Bay

There are many uses for biometric technology at California State University Monterey Bay (CSUMB), which is a small university on the Monterey Peninsula. CSUMB currently has approximately 4,000 students with 1,200 students currently living in residential halls on campus. The campus opened in 1995 and its growth has increased by approximately 500 students annually. According to a recently completed campus master plan update, by 2015 it is projected the campus will have approximately 9,000 students.¹⁸ Security of the dorm rooms, containing both female and male students, is of utmost importance to the students, their parents and the university. While stranger sexual assaults are rare on the CSUMB campus, nationwide sexual assaults are a concern at any college or university campus. In fact, federal crime reporting legislation known as the Clery Act was enacted in 1998. This legislation requires colleges or universities with certified police departments receiving state or federal funding to adequately document and report all Part I crimes and release the statistics annually to faculty, staff, students, prospective students and their parents.¹⁹

This federal legislation was enacted after Jeanne Clery, a student at Lehigh University in Bethlehem, Pennsylvania, was raped and murdered by a sexual offender who gained access to her dorm room while she was sleeping. The suspect gained entry into the residence hall via an unsecured outer door.²⁰

Unfortunately, lax site security is commonplace in residential halls in many colleges and universities, and CSUMB is no different. Biometric technology could be utilized at key entry points in residential halls utilizing biometric hand readers. This technology would eliminate any problems with unauthorized entry into the residential halls, thereby enhancing the safety of the students residing there.

Another biometric technology use at CSUMB could be the enhancement of building/classroom security. Currently, the university has a proximity reader alarm system with a magnetic lock at all doors leading to classrooms, administrative offices, meeting halls, lecture forums and all other buildings on campus. The door to these buildings open when an authorized user presents a key fob or alarm card. The issue with this is that key fobs or alarm cards can be shared or provided to non-university students which can allow an unauthorized access. Biometric technology, specifically hand reader technology, would be an enhancement to the existing system because the system would know specifically who was requesting entry. If an unauthorized person attempted entry into the building that had biometric hand reader technology, entry would be denied.

CSUMB is a computer technology-oriented university. Computer security for information systems that would prevent unauthorized use is another area that could benefit from the use of biometric technology for identification and verification. An individual could gain access to the university information system and ease the log-on

process by providing a fingerprint. Using this concept, when the fingerprint on the mouse or keyboard match the fingerprint that is already on file, the individual is allowed access to the information system.

Conclusion

Because of the challenges facing small university police agencies with limited resources, implementing biometric technology to enhance site security poses great challenges. However, the safety of the students, faculty and staff should be a priority. Biometric technology can enhance site security at CSUMB by not allowing unauthorized access to those who may be looking to commit crimes or prey upon students, faculty or staff. Collaboration and cooperation during biometric technology site security development on campus may reduce privacy concerns expressed by civil libertarian groups and the students, faculty and staff. Cost concerns of the biometric technology will have to be addressed through annual budget requests, to include seeking out grant funding and collaborative partnerships with private enterprise. Costs will vary depending on the specific technology used. Chapter III will address resources needed for a proposed strategy.

In the following chapters, the major hurdles facing the implementation of biometric technology that enhances site security are examined. Alternative strategies and implementation plans for successful integration of biometric technology are also examined. The next chapter introduces future forecasting through a facilitation process of the Nominal Group Technique (NGT).

CHAPTER II

FORECASTING THE FUTURE

The purpose for forecasting the future is to provide the opportunity to examine alternative futures, select a course of action, and then systematically set out to influence or shape the future. In any case, the process enables those who enlist it to better prepare themselves and their organizations for the inevitable changes that will occur in the world, with or without their influence. These objectives do not just occur. They require sustained effort and a systematic approach utilizing strategic planning and transition management techniques.

Forecasting facilitates these processes by supplying enough baseline information that, when combined with judgment and intuition, allow for the future to be managed as successfully as possible. When forecasting the future, it is important to remember that “what may be” must be viewed as a possibility, not a probability. In order to forecast the future of the impact that biometric technology will have on site security in a small university police department, a Nominal Group Technique (NGT) was employed.

Utilization of the Nominal Group Technique

A Nominal Group Technique (NGT) is a structured group process, usually facilitated by a third party, which identifies the major problems affecting or of concern to the group. NGT processes are geared toward issues involving judgmental or creative decision making. An NGT allows for maximum feasible participation by group members in the decision making process by avoiding the dominance of the group output by strong personality types and allowing all participants the opportunity for influencing the

direction of the group decision outcome.²¹

The NGT panel met in March 2004 and consisted of eight members from diverse backgrounds within the CSU Monterey Bay system. The panel included the associate director of information systems and network services, the student body president, a police lieutenant, an investigations sergeant, the assistant director of residential life, a transportation and parking administrator, a security systems services/locksmith manager, and the director of business and support services/risk manager (see appendix A).

Prior to the NGT panel being convened, each participant was provided with an informational packet containing background material concerning the potential use of biometric technology on a university campus relating to site security, the issue statement and a list of definitions (see tables 2.1 and 2.2). They were also provided a general overview of the NGT process, its purpose of identifying trends and events to assist in the development of a strategic plan, and the guidelines and procedures that would be used for forecasting both trends and events. In addition, the participants were asked to identify individually several trends and events prior to the scheduled NGT. The complete list of trends can be found in appendix B, and events in appendix C.

Strategic Purpose and Definitions

The purpose of this Nominal Group Technique exercise was to identify trends and events that could impact the strategic purpose statement. The trends and events were predicated on if biometric technology is implemented for site security at CSUMB. The panel was told that biometric technology, specifically hand readers, are advancing to the point that they may be available for site security in a university setting in the next three years.

STRATEGIC PURPOSE STATEMENT
How will biometric technology impact site security in a small university police department by 2009?

Table 2.1

DEFINITIONS
<p><u>Biometric Technology</u>: Refers to the automated capture of a person’s unique biological data that distinguishes him or her from another individual. Biometrics can be measured in many forms, including: fingerprints, voice patterns, iris patterns, hand geometry and facial features.</p> <p><u>Trend</u>: The occurrence of several similar events that take place over a short period of time and are indicators of possible change.</p> <p><u>Event</u>: Forecasting possible events in the future.</p>

Table 2.2

Trend Summary

During the NGT session, the panel members were asked to consider what trends they believed could impact the issue. The question presented was: “How will biometric technology impact site security in a small university police department by 2009?”

The panel members were led through the standard NGT process consisting of silent idea generation, round robin idea verbalization, group clarification, voting, ranking, and discussion of results. Appendix B reflects a complete list of candidate trends. The identified trends that the group believed could most impact the issue are presented in table 2.3.

TREND SUMMARY TABLE						
		1	2	3	4	5
	TRENDS	-5 Years	Today	+5 Years	+10 Years	Concerns (1-10)
T1	Level of campus security measures	40	100	125	135	8
T2	Expectation to provide safe environment	90	100	125	135	9
T3	Level of security convenience	50	100	150	170	7
T4	Level of identity theft	15	100	175	225	10
T5	Cost of technology	90	100	100	90	5
T6	Acceptance of intrusiveness of enhanced technology	50	100	125	135	5
T7	Interconnectivity of various data bases	10	100	150	150	4
T8	Speed of technology advancement	75	100	150	175	7
T9	Level of standardization with biometric technology	0	100	135	125	2

Table 2.3

The values in columns 1, 3 and 4 represent the panel’s subjective evaluation of the trend with Column 2 (“today”) representing the reference value of 100. The value in column 5 represents the panel’s concern (1-10) for the trend’s impact on the issue with 10 being the most significant. All values were calculated using an average of the panelists’ ratings.

A further analysis of the trends discussed by the panel members is as follows:

1. Level of campus security measures

Site security is something that is on the minds of nearly everyone in light of September 11, 2001 and the heightened awareness of the potential for terrorist acts. The panel forecasted that biometric technology could enhance site security on campus and that students, staff, faculty, and visitors to the campus

would be tolerant of the enhanced security measures due to the overall perception that site security is a priority for everyone in this day and age, not only on university campuses, but nationwide as a whole. In assessing the trend, the panel concluded that the level of security was significantly less five years ago than it is today. The panel projected the level of security will increase by twenty five percent in five years, and increase only slightly more between years five and ten. The panel assigned a level of concern of eight to the trend because there will always be concern about security on campus and this should support the proposal for biometric technology.

2. Expectation of CSU Monterey Bay to provide a safe environment

The faculty, staff, and students believe that the university as a whole has a duty and an obligation to provide a safe and secure environment on campus. The panel forecasted that the site security expectations of students, staff, and faculty will continue to rise with the advent of these types of technological advancements relating to site security. With federal legislative efforts such as the Clery Act, which is intended to inform students about criminal acts in and around their campus, the demand to provide and enhance site security in a university setting will continue to grow. The panel felt the expectation to provide a safe environment was slightly less five years ago, will be twenty five percent higher in five years and continue to rise in ten years. The panel assigned a level of concern of nine to the trend indicating that there will always be a high expectation from faculty, staff and students for the university to provide the safest environment possible. This will also lead to support for

biometric technology security measures.

3. Level of security convenience

Using the existing campus security system as an example, students, faculty and staff have utilized a system called a proximity card reader for access into buildings and residential halls for about nine years. A card, similar to a credit card, is needed to access the various buildings on campus. Biometric technology would eliminate the need for users to carry an entry card, leading to convenience for those desiring entry into a building. The panel forecasted that the convenience a biometric site security system could provide would be a positive selling point that may equate to buy in from users. They felt security convenience would increase by fifty percent in five years and continue to increase slightly in ten years. The panel assigned a level of concern of seven to the trend, because implementation of biometric technology would be critical to this improvement.

4. Level of identity theft

Most of the general public is aware of the increasing amount of identity theft. There is an overall awareness that measures have to be taken to combat the identity theft issue. The panel thought that the trend of identity theft was significantly less five years ago than what it is today. Without some intervention such as biometric technology, the panel projected that identity theft will almost double in five years and will more than double in the next ten years. This trend was selected by the panel as the highest level of concern

(ten) out of all the trends identified, which emphasizes the need for security measures such as biometric technology. The panel felt that biometric technology would be a positive tool in addressing the issue of identity theft. The introduction of biometric technology for site security purposes would allow the public to become familiar with this technology. Familiarization of this technology could easily dovetail into other areas of society, such as the increase in identity theft/fraud incidents, which is placing a burden on law enforcement agencies to investigate such incidents.

5. Cost of technology

The cost of converting to site security biometric technology at CSU Monterey Bay at the present time is cost prohibitive based on the current state of the budget woes facing California. This factor alone could determine if this type of technology is considered for use on campus. The panel believed that as the public becomes familiar with this technology and it is utilized for such purposes as site security, the biometric technology industry will become more competitive and the cost to implement a biometric technology system for site security will become more affordable. In assessing the trend, the panel believed that the cost of this technology will remain high between today and the next ten years, with a ten percent decrease in cost within ten years. They felt that as a result of the industry becoming more established, biometric technology firms will compete for customers, which will lower the cost, thus the panel only had a mid-level of concern regarding its affordability.

6. Acceptance of intrusiveness of advanced technology

The panel generally believed that society is becoming more accepting of technological advancements relating to security enhancements, whereas previously, mention of technology such as biometrics may have conjured up thoughts of government intrusion or big brother is watching. Over time, the panel felt that biometric technology will integrate nicely into society and become a way of life. They thought this trend would increase by twenty five percent in five years and continue to increase slightly in ten years. The panel had a mid-level of concern with this trend since they believed as technology advances in society, intrusiveness becomes more acceptable.

7. Interconnectivity of various databases

The panel saw concerns with users currently having multiple passwords and access cards as it relates to site security. The panel believed that one main database with identifying information utilizing biometric technology is a trend that would be very beneficial and could streamline the need to maintain numerous forms of identification, access cards and passwords. In assessing the trend, the panel concluded that the level of interconnectivity of various databases was significantly less five years ago than it is today. They felt it would rise by fifty percent in the next five years and remain level between years five and ten. The panel thought that as specific technology databases become more established, there will be less of a need for various databases, therefore the panel had a concern level of four with this trend.

8. Speed of technology advancement

The panel members believed there is a trend in today's highly advanced technology age that new technology is becoming obsolete in a much shorter time frame than in years past. This trend can pose a problem for governmental agencies that historically have a lengthy research and implementation process. When exploring the need for new technology it can become obsolete shortly after purchase and implementation, or even before. The panel concluded that the level of technology advancement was twenty five percent less five years ago than what it is today, will be fifty percent higher in five years, and will continue to advance in ten years. The panel assigned a level of concern of seven to the trend, indicating that it was important to the issue.

9. Level of standardization with biometric technology

The panel believed that as biometric technology matures and gains in popularity, there will be a trend to standardize or streamline the specific areas of biometric technology as it relates to site security and other areas where the technology could be useful. In assessing the trend, the panel scored the trend as non existent five years ago, giving it a value of zero. They thought the level would increase thirty five percent five years from today, and interestingly enough will slightly decrease between five and ten years. The panel's reasoning for the decrease was that the standardization of this technology will peak in five years and then it will see a decrease as other technology is introduced for site security. The panel assigned a level of concern of two to the trend, indicating they thought its impact on the issue is quite positive.

Event Summary

Following the discussion on trends, the panel members were asked to consider the following question: What events – either positive or negative – will impact the implementation of biometric technology as it relates to site security in a small university police department by 2009?

For a second time, the panel was led through the standard NGT process of silent idea generation, round robin idea verbalization, group clarification, voting and ranking and discussion of the results. The identified events that the group believed could most impact the issue are presented in Table 2.4. A complete list of events can be found in Appendix C.

EVENT SUMMARY TABLE					
		1	2	3	4
	EVENTS	Year >0	+5 Years	+10 Years	Impact + or - (1-10)
E1	Terrorist attack a CSU campus	2	85%	95%	+7
E2	Legislation mandating implementation	3	75%	90%	+5
E3	Network virus	1	75%	75%	+5
E4	Serial Rapist	2	90%	95%	+8
E5	CSU mandates system wide security standards	5	20%	45%	+6
E6	Identity theft	2	40%	50%	+2
E7	Database info misused	2	75%	80%	-2
E8	Systems failure	2	20%	20%	-2
E9	Mentally deranged suspects actions thwarted	3	10%	10%	+5

Table 2.4

The values in Column 1 represent the panel's determination of the first year the probability of the events occurring exceeds zero. The values in Columns 2 and 3 represent the panel's determination of the event's probability (0% to 100%) of occurring within five and ten years, respectively. The value in Column 4 represents the positive or negative magnitude of the event's impact on the idea. All values were calculated using an average of the panelists' ratings.

A further analysis of the events discussed by the panel members is as follows:

1. Terrorist attack on a CSU campus

Since September 11, 2001, terrorist attacks are on the minds of all Americans. Biometric technology was discussed as a safeguard against future attacks, particularly the so called "soft target", such as educational institutions . Any future terrorist attacks would lessen resistance to widespread use of biometric technology for site security. The panel thought that a terrorist attack similar to September 11, 2001 could first occur in two years, with educational institutions being potential targets. The probability of a terrorist attack on a CSU campus was 85 percent in five years, increasing to 95 percent probability in ten years. The impact of this event on the issue is a positive seven, indicating that while terrorist attacks on educational institutions with the magnitude of the September 11, 2001 attacks would be catastrophic, it would bring to the forefront the need to implement this technology for site security.

2. Legislation passes mandating implementation of biometric technology
Legislation is passed which requires California state universities to implement biometric technology into site security. It was felt that as biometric technology becomes more prevalent in society, there may be legislative mandates requiring public institutions to implement the technology. The panel felt that the earliest this could occur would be three years, particularly if educational institutions are specifically targeted by terrorists or if attacks occur. The panel thought there is a seventy-five percent chance this could occur within five years and increasing to a ninety percent chance within ten years.

3. Computer network virus infects CSUMB information technology database
The panel felt that a computer virus could potentially impact the database developed for biometrics, leading to catastrophic consequences with database information. While the panel believed a virus would initially have a negative impact on the success of this technology, they also believed the impact would be positive because there would be more of a monetary investment in upgrading the system to prevent such a virus in the future. They believed the earliest this event would occur is one year, with computer network virus being commonplace in the computer age. The panel thought that there is a seventy-five percent chance of this occurring within five years and the probability does not increase in ten years. The impact of this event on the issue was a positive five, with the panel suggesting that a network virus would cause the database system to

be upgraded to avoid any future occurrences.

4. Serial rapist selects CSUMB to commit sex crimes

A serial rapist selects CSU Monterey Bay to sexually assault female students in their dorms, in isolated classrooms or study halls. The panel felt that an event of this magnitude could occur within two years at the earliest, with a ninety percent chance of it occurring within five years and a ninety-five percent chance within ten years. The impact of this event on the issue was a positive eight. The panel felt a crime of this nature would have a significant positive impact on the development and implementation of this technology for site security.

5. California State University system standardizes site security systems

CSU Monterey Bay is one of twenty-three campuses in the statewide university system. It was thought that if the Chancellor (who oversees all twenty three campuses) mandated biometric technology as a standard for site security on all campuses, then this technology would be commonplace on all CSU campuses statewide. This discussion presumed the technology would be available. The earliest the panel thought this event would occur was in five years, with a twenty percent chance of it occurring in that five year window, and forty-five percent within ten years. The impact of this event on the issue was given a positive six, although the panel did have some skepticism that the event could or would actually occur.

6. Significant identity theft on campus

This event is defined as a university employee accessing the existing data base and retrieving student, faculty and staff identifying information (date of birth, address, and social security number) for the purpose of committing identity theft with the intent to fraudulently obtain credit cards. The panel felt that if a crime of this nature occurred and biometric technology was available to the campus as a means of minimizing the need to have common identifiers, it would be a positive step in implementing this technology campus wide and perhaps CSU system wide. The group felt that this could occur within two years, with a forty percent chance of it occurring within five years and a fifty percent chance in ten years.

7. Biometric technology database information misused, violating citizens' rights

The panel noted that some federal or military agencies currently have access to biometric technology databases. The panel believed that if these agencies misused identifying information obtained from biometric technology databases in violation of the Patriot Act, this type of action could have a detrimental effect on the future use of this type of technology. The Patriot Act was developed as a result of the 2001 terrorist acts against the United States as a means to permit monitoring of activities of those who may be engaged in harmful activities against the United States. The Act is under constant scrutiny by the public and if there

was an unauthorized access by law enforcement personnel of data associated with this technology, public support of this technology may be damaged. The panel believed this could first occur in two years, and there was a seventy-five percent chance of this occurring within five years and an eighty percent chance within ten years. The panel believed this event would have a negative impact on the issue, rating it a negative two.

8. Computer database system containing biometric data crashes

The panel believed that a major system failure of a computer system containing biometric technology data at a location that is experimenting with this technology would have a negative impact on the CSU system implementing this technology at any of its campuses, specifically CSUMB. The panel felt that that the earliest this event might occur would be in two years, with a twenty percent chance of it occurring within the next five to ten years. The impact of this event on the issue was a negative two, indicating that a major system failure would have a negative impact on the implementation of this technology.

9. Mentally deranged suspect's actions thwarted with biometric technology

The panel defined this event as a disgruntled ex-employee with mental problems who is denied access to a science building in a large east coast university because his biometric data has been removed from the data base, which denies him access to the building. The suspect is armed with an assault rifle and has plans to go on a murdering spree at the university.

He is apprehended by university police officers before he can harm anyone; he is fleeing the area because he was denied access to the building as a result of his data being removed from the biometric database. The panel felt that an event of this nature could occur in three years at an educational institution that is visionary with implementing this technology for site security but gave it an overall probability of only ten percent of occurring within ten years. The impact of this event on the issue was a positive five. The panel felt that if an event of this magnitude was thwarted by the use of this technology at another university, biometric technology systems would gain popularity and acceptance at other educational institutions.

Cross Impact Analysis

After identifying the trends and events that could impact this issue, the panel was then asked to consider the following questions: If an event occurs, what effect will it have on a trend? Will that impact have a positive or negative effect on the issue? The cross impact analysis identifies the positive or negative impact of an event occurring and is presented in Table 2.5 by using a scale of -10 to +10, again using an average of the panelists' ratings.

CROSS IMPACT TABLE									
EVENTS	TRENDS								
	T1	T2	T3	T4	T5	T6	T7	T8	T9
E1 - Terrorist attack on a CSU campus	+7	+7	-5	0	-5	+8	+5	+5	+4
E2 - Legislation mandating implementation	0	+8	-3	+4	0	0	0	+2	+3
E3 - Network virus	+3	+2	-5	-8	-3	-6	+4	+5	-5
E4 – Serial rapist	+7	+7	-6	0	0	+8	0	+2	+2
E5 - CSU mandates system wide security standards	+8	+8	-5	0	+8	-2	+3	-3	+8
E6 - Identity theft	+5	+8	-4	+8	-3	+6	+7	+5	+4
E7 – Database info misused	+3	+8	-3	0	0	-1	+5	+5	+8
E8 - Systems failure	0	+4	-8	0	0	-8	0	+5	+8
E9 - Mentally deranged suspect’s actions thwarted	+8	+8	-8	-8	0	-8	-8	+8	0
Trend 1 – Level of security measures Trend 2 – Obligation to provide safe environment Trend 3 – Level of convenience Trend 4 – Level of identity theft Trend 5 – Cost of technology Trend 6 – Acceptance of intrusiveness of enhanced technology Trend 7 – Interconnectivity of various data bases Trend 8 – Speed of technology advancement Trend 9 – Level of standardization with biometric technology									

Table 2.5

Upon examination, Table 2.5 indicates that a large scale terrorist attack on multiple government buildings (event one) would have a positive impact on most of the trends. This could lead to a wider use of biometric technology for site security, particularly at universities, which are often referred to as “soft targets” when used in the context of projecting the targets of future terrorist attacks.

The passage of legislation requiring implementation of biometric technology at all California state universities (event two) and the CSU system mandating system wide

security standards (event five) would have a positive impact on the expectation of CSU Monterey Bay to provide a safe and secure campus environment (trend two). The panel felt that if biometric technology was mandated for site security at all CSU's, either by legislation or by the system wide chancellor, it would probably come with funding for each campus to implement a biometric technology site security system.

The panel viewed a computer network virus infecting information technology containing biometric technology data (event three) as negatively impacting the convenience of having such a system (trend three). It could also lead to the public being less accepting of the intrusiveness of this technological advancement (trend six), who were probably skeptical of the technology to begin with.

Event four (serial rapist) positively impacted trend one (level of security measures), trend two (expectation to provide a safe environment) and trend six (acceptance of intrusiveness of enhanced technology). The panel believed that if a serial rapist targeted the CSU Monterey Bay campus and committed sexual assaults, campus community members would welcome a biometric technology enhanced site security system and they would be more accepting of the perceived intrusiveness of this type of technology.

The panel felt that if the CSU system mandated system wide security measures at all CSU campuses(event five), it would have a very positive impact on several of the trends, most notably trend one (level of security measures), trend two (expectation of the university to provide a safe environment), trend five (cost of technology) and trend nine (level of standardization with technology).

Futures Scenario

Information that was developed through the literature research, as well as information derived through the NGT forecasting process, was blended as a basis for developing three scenarios of possible futures or alternative futures regarding the issue statement. These are presented as a pessimistic scenario, an optimistic scenario, and a surprise free scenario.

Scenarios are future stories used to play out trends and events as identified by the NGT panel and are based on information surrounding the issue as identified in Chapter One. They are provided as “what if” models and are designed to highlight the changes that could occur based on the identified trends and events. A pessimistic scenario is not viewed as a positive outcome and is to be avoided if possible. The optimistic scenario is where law enforcement would want to be regarding the issue, but may be unlikely, given the potential of organizational and university community resistance to biometric technology. A surprise free scenario may not be the most desirable alternative future, although it may be the most likely.

Pessimistic Scenario

The year is 2009 and several university campuses across the United States have been the scene of terrorist bombings and biological attacks. There have been injuries and deaths of faculty, staff and students associated with these attacks. Fueled by several of these high profile incidents, the public is growing increasingly impatient and concerned with campus police and university administrators nationwide with their inability to effectively protect campuses from these terrorist incidents.

To reassure a weary public, in 2007 the California legislature mandated that by 2009, all California State Universities system wide will have biometric technology installed for site security on all campuses with the hope of preventing these violent incidents from occurring. A key component to implementing the technology at all campuses system wide, to include CSU Monterey Bay, is the required funding for the purchase of these systems. Unfortunately, these terrorist attacks are widespread nationwide. State and federal funding is being spent on attempts to protect our borders, airlines and mass transit from terrorist attacks, therefore no Homeland Security Grant funding assistance, or any other grant funding sources, is available.

To add to the difficulty of being unable to fund a biometric technology site security system, the CSU Monterey Bay student body association and the statewide teachers association is opposing the installation of such a site security system. They believe this technology is an invasion of privacy. They have solicited the assistance of the American Civil Liberties Union, which on behalf of the students and faculty, has filed a lawsuit to prevent the installation of a site security biometric technology system on the CSUMB campus.

Optimistic Scenario

In 2009, the CSU Monterey Bay Police Department was successful in the planning, research, development and implementation of a site security biometric technology system at the university. The technology is utilized by students, faculty and staff to gain access to buildings, classrooms, lecture halls, residential halls and virtually all other buildings throughout the campus.

Within three months of installing the biometric technology site security system,

university police officers were notified by dispatchers at the university communications center of a high risk sex offender attempting to gain entry into a female only residential hall. The suspect had previously submitted his biometric data to a nationwide database as a term of his release from prison and parole. The security system does its job and doesn't allow the suspect to enter, who presumably has intentions of committing a sexual assault. Responding bicycle officers see the suspect as he attempts an escape, and he is apprehended after a short chase. The technology is funded through a combination of state and federal grant funding.

Within one year of installing the biometric technology site security system, CSU Monterey Bay realizes a 65% decrease in thefts and burglaries from buildings on its campus. The university is well known and popular for its computer education courses. Many computer thefts were committed prior to the installation of the system. The reduction in thefts of university computers and other equipment allows the university to utilize precious financial resources to educate the students instead of replacing equipment that was stolen prior to installing the site security system.

Surprise Free Scenario

The year is 2009 and university police departments across the nation have been instrumental in the implementation of biometric technology site security systems on their campuses. Forced to become more efficient with site security due to an increase in property crimes and the fear of terrorist attacks, university administrators have recognized the importance of these site security systems and have secured state and federally funding for the installation of these systems throughout the 23 CSU campuses.

This technology, however is not without its critics. The ACLU has made several

attempts to block the installation of this technology claiming it violates California's Constitutional guarantee against the governments invasion of privacy. The statewide university police association and its members have resisted this technology, since they believe it will reduce the crime rate at campuses system wide, relating to fewer officers that will be needed to police university campuses.

Many private site security firms, large and small, have benefited from the popularity and use of biometric technology systems for site security. Most of the technology systems being sold to large institutions like CSU Monterey Bay are being designed and manufactured exclusively outside the United States. Subsequently, the price of these technology systems has dropped dramatically in the past couple of years. While this could be viewed as positive from the perspective that these technology systems have become very affordable, there is currently a lawsuit pending by a United States biometric technology firm alleging they should have the right to sell their technology system to CSU Monterey Bay, instead of the system that the university was planning on purchasing from a non U.S. firm.

Why Look Ahead?

Research and NGT forecasting indicates that biometric technology could have an impact on site security and university police departments in the near future. As illustrated in the alternative future forecasting, the impact can be either positive or negative.

No one can predict the future, although by actively participating in future studies, leaders may be able to foresee trends and events that impact them. Writing alternative scenarios, while awkward at first, allows for deep analysis and offers a creative method

for dealing with situations before they come to fruition. This process allows leaders to formulate alternatives to problems before they occur. When utilized effectively, futures studies can be an integral component of meaningful strategic planning. Scenario development is but one aspect of the strategic planning process, which will be discussed in the next chapter.

CHAPTER III

STRATEGIC PLANNING

Strategic Planning

Strategic planning is a systematic approach to create and manage a desirable future. The purpose is to provide a structured approach to issues that an organization will face in the near future. Many times this process is used to determine if the organization is moving in the desired direction and if its programs are receiving the necessary resources, proper funding, and to establish operational goals, enhance cooperation among its divisions, and ensure consistency and accountability throughout the organization.

There are five steps to this planning process: 1) selection or identification of the organization's mission and major goals; 2) analysis of the organization's external competitive environment to identify opportunities and threats; 3) analysis of the organization's internal operating environment to identify strengths and weaknesses; 4) selection of strategies that build upon the organization's strengths and correct its weaknesses in order to take advantage of external opportunities and counter external threats; and 5) strategic implementation.²²

The surprise-free scenario presented in Chapter II was chosen as the basis for developing a strategic plan. When developing and implementing a biometric technology site security system, failure to focus on a funding source for this technology and the potential resistance of this technology on a university campus by students, faculty and staff would be detrimental to the successful implementation of such a system.

External Environment Situational Analysis

In order to anticipate the impact that biometric technology will have on site security in a small university law enforcement agency by 2009, it is important to first examine those areas that may have the greatest effect. This can be accomplished by scanning Social, Technological, Environmental, Economic, and Political issues, otherwise known as STEEP. External forces and environment will affect the strategic planning process. Before developing an effective plan for implementing biometric technology for site security in a university setting, the law enforcement leader should conduct an analysis of the external environment to identify threats and opportunities. The following are examples of issues to consider while conducting such an analysis:

Social:

- Biometrics has no established governmental protocols or use.
- No industry standards have been implemented for this technology.
- Society as a whole is suspicious of biometric technology.
- University students and their parents demand a safe and secure learning environment, particularly in dormitories or residential halls.
- As the use of biometric technology becomes more common in all facets of everyday lives, public mistrust of this technology should diminish.

Technological

- Biometric technology with an associated data base can be susceptible to hackers.
- As with any technology, mismanagement will result in undesired and/or unanticipated consequences.
- Biometric technology is not currently at a stage for widespread use, although it is anticipated that will change in the near future.

- Technological advances in biometric technology and data storage will allow for greater use by law enforcement, to include site security in a university setting.

Economic

- Since biometric technology is relatively new to law enforcement, the economic impact for acquiring this technology for site security is untested.
- With increased interest in this technology, competition in the market and consumer demand may dictate the price structure of the technology.
- State and Federal Homeland Security grant funding may be available for the implementation of biometric technology for university site security purposes.

Environmental

- Special interest environmental groups who disagree with implementing this technology at a university may engage in vandalism of the biometric scanning equipment used for site security.
- Biometric scanning devices may have a negative visual impact on the campus environment.
- It is unknown what health effects (if any) a wireless or wired biometric system can have on those exposed to the technology.

Political

- University political leaders will weigh economic costs and potential student resistance when deciding to implement biometric technology for site security.
- The overarching goal of providing security and safety to all that utilize the university campus should gain widespread political support.
- Segments of students, faculty and staff at the university may perceive biometric technology as an infringement of their civil liberties.

Organization Analysis – Strengths and Weaknesses

An important component of any strategic plan is an organizational analysis that examines the strengths and weaknesses of the organization using the issues discussed in

the STEEP model. The comparison of the organization's external opportunities and threats, and its internal strengths and weaknesses is referred to as a SWOT (strength, weakness, opportunity, threat) analysis. The SWOT analysis typically encompasses the STEEP model as a reference framework. "The central purpose of the SWOT analysis is to identify strategies that align, fit, or match an organization's resources and capabilities to the demands of the environment in which it operates. Put another way, the purpose of the strategic alternatives generated by SWOT analysis should be to build on an organization's strengths in order to exploit opportunities, counter threats, and correct weaknesses."²³ Weaknesses are potential internal challenges where the organization needs to focus. Using the California State University Monterey Bay and its police department as a model for the future impact of biometric technology on site security at a small university by 2009, the following questions were considered while conducting this analysis:

Strengths:

- CSU Monterey Bay is one of the newest universities in the CSU system. Opened in 1995, the university is well known for its technology programs.
- There is a strong organizational commitment to providing the safest learning environment.

Organizational Weaknesses:

- Law enforcement efforts on university campuses, including CSUMB, have historically been viewed by administrators as security guards, therefore law enforcement efforts are mostly reactive instead of proactive and as a result, campus law enforcement may not be as forward thinking as it could be.

Opportunities:

- The campus community views its university police department as very professional and innovative.
- Technology grants may be available through state and federal homeland security grant funding.
- There is a heightened level of public safety, personal security and facility security on campus.
- The campus community is supportive of community policing efforts

Threats:

- The State of California is currently in its worst budget crisis ever. While the economy appears to be improving, it is unknown how long the economic recovery will take, which could have long term impacts on implementing new technology.
- There is a general lack of knowledge in both public and private sectors regarding biometrics and how the technology can serve as a useful tool.
- Civil libertarian organizations' resistance may be strong against biometric technology, and they would most likely mount a public campaign or legal challenge against its use on a public university.
- A cost effective biometric technology site security system is not immediately available, although the cost of this technology is expected to decrease in the future due to increased competition with vendors. It is projected that an affordable biometric technology site security system will be available in five years.

Stakeholder Identification and Analysis

Stakeholders are groups or individuals who are either impacted by what we do, or impact what we do as an organization. Prior to any attempts to develop strategic alternatives, it is critical to identify stakeholders, who may be internal or external to the organization and are interrelated in many ways. Stakeholders are in a position to oppose, support, or be indifferent to the change issue, depending on their own perspectives.

Several of the stakeholders who could have a role in the development and implementation of a biometric technology site security system at CSU Monterey Bay may include:

- Chancellor of the statewide university system: The chief executive officer of the twenty three university system. Has the ability to initiate new technology throughout the CSU system. Has impact on implementing new technology and new policy. Is influential with policy makers outside the organization, such as state and federal officials. Is concerned with the safety of all who utilize campuses in the CSU system and is supportive of new technology that will accomplish that goal.
- President of the university: The CEO for an individual campus. Has the ability to set and impact policy direction on campus, relies on input from his cabinet regarding the implementation of new technology. Has a responsibility as CEO of the campus to ensure his university is a safe environment, while at the same time balancing the financial costs of a site security system with site security needs. Is supportive of new technology that will enhance site security.
- University President's cabinet (chief of staff, provost, vice presidents): These individuals provide input into the implementation of policy and provide direction to the overall operation of the university. They are supportive of new technology that will enhance campus site security.
- University police chief: Sets the vision for the operation of police services on campus. Historically relies on police managers and supervisors to develop operational plans for line level personnel. Has an interest in keeping crime to a minimum on campus and is supportive of new technology that will accomplish this.
- University police department command staff and supervisors: Some of these managers and supervisors may not be supportive of new technology, while others may be supportive of the concept. They are directly responsible for policy and procedure development regarding day to day operations.
- University security system analysts: These individuals are the technicians that operate the site security system on campus. They may lack experience or knowledge with biometric technology and may not be supportive of its implementation.
- University chief information officer and his staff of information technology employees: The individuals who are critical to the development, implementation and maintenance of the biometric technology database. They are generally

supportive of technology advances with site security, although they can also see view biometric technology as an increase in their technology workload.

- Students and their student council: These are the individuals who the university police department serves and protects. The students generally are supportive of law enforcement efforts to enhance campus community safety. They may however, see the university police department's proactive efforts with implementing biometric technology as overreaction and an invasion of their privacy.
- California State Employees Association (CSEA): The CSEA is the union that represents non-management staff employees in the CSU system, which includes administrative assistants, facility repair employees, and maintenance workers, and all other non-faculty employees. While many of these employees may generally support this technology and see it as an enhancement of their safety in the workplace, others may view it as an invasion of their privacy and oppose it.
- California Faculty Association (CFA): This association represents all faculty members in the CSU system. Like the CSEA, many faculty members may generally support this technology in the interest of their safety in the workplace, while others may view the technology as an invasion of their privacy and oppose it.
- Biometric technology infrastructure vendors: These are the individuals and privately owned businesses that are critical to the development and implementation of site security biometric technology systems. They are obviously supportive of this technology since they will benefit financially from the sales and installation of biometric technology site security systems.
- Civil libertarian organizations: These are the groups (or individuals) who have spoken against the use of biometric technology in society and are viewed as potential adversaries.

Often overlooked during this analysis are potential snail darters, who are unanticipated stakeholders that can impact an issue. Snail darter is a term that has come to mean those who may not initially be considered to be a stakeholder but ultimately they can become a roadblock if their concerns are overlooked or not considered. It is important to take these individuals into consideration when developing a strategy for change.

Regarding biometric technology for site security, these snail darters may surface

as right to privacy groups, such as the American Civil Liberties Union, National Urban League, Human Rights Watch, et cetera, who generally oppose the use of technology in society or they perceive infringement on personal freedom.

Development of Alternative Strategies

The next step of the strategic planning process requires generating a series of strategic alternatives that builds upon the organization's strengths and corrects its weaknesses in order to take advantage of external opportunities and counter external threats. The strategies proposed should be designed to bring about a desired future as envisioned. Based on research as well as the results of the NGT process, three alternative strategies were developed relating to the implementation of biometric technology for site security at California State University Monterey Bay. Each of the following three strategies represents varying levels of the impact and approaches to biometric technology on site security.

Strategy One – Do not implement biometric technology for site security purposes

This strategy is indifferent to the issue. Although this strategy is the easiest and will generate the least resistance of the three, it is not a proactive approach to implementing biometric technology for site security. While the possibility exists that as this technology grows in popularity, it may become more accepted by those opposing its implementation in a university setting, although there are no guarantees this will occur.

Strategy Two – Gradual introduction of biometric technology for site security

In this strategy, the organization gradually introduces biometric technology for site security, concentrating at first on areas where there will be the least resistance by

those opposed to this technology. Residential halls/dormitories would be the likely choice for minimal resistance. Although student, faculty and staff involvement is minimal at this point, the police leader should take the opportunity to gauge support of the technology and plan for future expansion of the technology to other buildings on campus. The university police department can concentrate on converting existing proximity card reader security systems to biometric technology and phasing in this new technology.

Strategy Three – Implement a biometric technology site security system campus wide

This strategy involves a very strong leadership role for implementation of this technology campus wide on all buildings. Strategy three clearly involves the most work and the highest level of commitment on the part of the university police department's leader and the policy makers of the previously identified stakeholders. This is also the strategy that may meet with the most resistance and will be the costliest.

The police leader will have to develop and cultivate broad based campus support, to include convincing the university president and his cabinet that the technology is worth the commitment of substantial financial resources. This could be a daunting effort, particularly in difficult financial times, and if handled improperly has the potential to derail the entire concept or plan. It is recommended that this approach only be followed if there are urgent issues that need to be addressed requiring immediate action, such as multiple violent crimes being committed against students, faculty or staff on campus.

Selection of the Appropriate Strategy

Alternative strategies are dependent upon many different variables. They depend upon the particular organization, the external environment, and the issue(s) contemplated. In the selection of a specific plan, the organization and campus community

will need to assess not only their level of need, but also the strengths, weaknesses, opportunities and level of resistance of the various stakeholders. When contemplating a particular strategy, it is also important to focus on the issue statement, “How will biometric technology impact site security in a small university police department?” As previously stated, the cost of such a site security system is going to be a primary factor which will require the police department leader, the university president and his cabinet, to assess resources and estimate initial and ongoing costs before any such site security system can be implemented.

Barring any major crime incidents on campus that requires urgent action, strategy two has the most appeal if cost is not a factor. It allows for gradual implementation at a pace consistent with the level of resistance and resources. The best chances to develop buy in from stakeholders, partnerships, collaborations, and shared vision regarding the implementation of this technology rests in an incremental approach. It is recommended the first step in an incremental approach would be the installation of biometric technology hand readers in residential halls on the CSUMB campus in lieu of the proximity card readers currently in use. Using this strategy as an example for a cost estimate, there are fifteen residential halls on campus housing approximately 1,600 students. Based on the existing hand reader technology available, it is estimated the cost to equip each common entrance of the residential hall will be \$25,000 per building, totaling \$375,000 to equip all residential halls on campus. It is expected this technology will be available and accepted in the next few years for use in a university setting.

The next chapter will discuss the incremental approach to organizational change utilizing strategy two and transition management.

CHAPTER IV

TRANSITION MANAGEMENT

Transition Planning

Prior to carrying out any transition plan, it is essential that law enforcement leaders fully understand the proposal. They must also ensure that they, and other key decision makers, are well versed in the facilitation of the plan and change process. Most importantly, they must be supportive of the plan and committed to seeing the proposed changes through to fruition. Assuming that the law enforcement executive of the university police department has the financial resources and the approval of the university president and his cabinet to proceed with the planning and implementation of a biometric technology site security system, focus can then be concentrated on bringing in the various stakeholders. The transition planning phase can be an enormous undertaking.

The following transition plan, using the CSU Monterey Bay Police Department as a model agency, is a very broad example of a small university police agency's implementation of a biometric technology site security system. During this phase, the law enforcement executive should take into account the uniqueness of providing such a site security system in a university setting, assess potential resistance of implementing such a system in a public university setting and be prepared to modify a plan that best suits the university community.

A biometric technology site security system will require various collaborative approaches requiring partnerships and mutual cooperation from the various stakeholders mentioned earlier. If the university or the stakeholders are not ready to change, then the most comprehensive strategic plan will not produce the desired results. Some questions

the law enforcement leader must ask and receive answers to are:

- What is the level of trust among the key stakeholders?
- What are the roles of the stakeholders?
- Have the stakeholders experienced working collaboratively in the past?
- Does the university have sufficient resources to implement a full or partial biometric site security system?

Establish Steering Committees

In any change effort, there is always at least one person who is key to the success of the project. The person in this role must be capable of providing leadership and should embody a vision to see the project through. Typically this person (sometimes referred to as the chairperson or project manager) will head a steering committee that acts as a change agent throughout the entire process. The project manager is critical to the success of the transition and oftentimes sets the tone for how the project will be facilitated.

Develop a Shared Vision

Developing a shared vision is crucial to the successful implementation of a biometric technology site security system. If leaders strive to be change agents, they must have a vision and impart that vision to others effectively. A vision that is frequently and enthusiastically shared with the organization's members will go a long way in garnering support from those that will share in making the project a reality. In any organization, it is human nature for people to maintain the status quo unless they become involved with organizational change. The vision (or desired future) must be clearly illustrated in a manner that is as appealing as possible. Once the vision is established, it must be effectively communicated throughout the organization, which will in turn, act as a

catalyst for the needed organizational change.

Foster Consensus

The implementation of any new technology can be a daunting task individually and organizationally. When implementing the selected strategy, timing, trust, shared vision, and buy-in are all critical for success. Identification of the key stakeholders was discussed earlier; now is the time to actively involve representatives from each of these groups with the ultimate goal of gaining consensus. Representatives should be involved on either the steering committee or other task groups and it is important to share with participants the change vision and other important key elements of the process. It is important to impart to stakeholders that they are constituents in the process, not spectators, opponents, or adversaries.

Share the Vision With Inclusiveness

With an organizational change needed to embrace the development and implementation of a biometric technology site security system in a university setting, it is important to determine the level of commitment necessary from those in the organization for the change to be successful. This may involve taking the time to examine the various levels of authority that exist to make the change possible. Many organizational leaders try to force change on their subordinates without giving consideration to the commitment needed from them. Giving stakeholders a sense of ownership creates buy-in and commitment to the project. In order to elicit the necessary commitment, it is important to have an understanding of the resistance that may prevail. The levels of commitment in organizational change are:

- Let it Happen
- Help it Happen
- Make it Happen

These commitment levels will be discussed further in the pages that follow.

Financial Resources Required for Implementation

The implementation of a biometric technology site security system will require a variety of funding sources. While initial funding for the project may come from state and federal Homeland Security grant funding, sustained funding may also be located in a partnership with the private contractor that manages the residential halls/dormitories on campus. Some of the costs associated with implementing such a site security system include equipment, training, administration, implementation and on-going maintenance of the system. State and federal grants are usually considered as the first source of funding for a project of this nature, particularly as a component of protecting a public university from a homeland security perspective.

The impact on a university law enforcement agency and the university in general with implementing a biometric technology site security system has the potential to be a monumental undertaking both monetarily and from potential resistance that may exist in the campus community and within the organization. The law enforcement leader proposing the project will have to demonstrate exceptional leadership and communication skills when articulating their vision of the positive benefits a biometric technology site security system can have on providing a safe and secure environment for students, faculty and staff.

Policies Required for Implementation

Once stakeholders are committed to implementing a biometric technology site security system, have an understanding of its capabilities, and are trained in its use, it becomes necessary to introduce policies, systems, and structures regarding the operation of the system. Policies will need to be drafted that govern the use of this technology and the ramifications of abuse of identifying data collected and stored in the system's database. Constant management monitoring of the system and follow up regarding its operation and reliability will ensure that this technology system will become an institutionalized tool that provides long term site security benefits to the university.

Transition Management and Critical Mass

Organizations seeking transformational change must recognize that in order for strategic transitional plans to be effective, proper leadership of the transition itself must occur. Though several essential elements of the change process have already been discussed, it is necessary to examine other critical aspects that are more relative to setting the stage for change. Leaders within organizations who accept the change challenge must be cognizant of and understand the principals of critical mass as it relates to the change process. Critical mass is defined as the minimum quantity of specific individuals or groups who, if they actively support the proposed change, will insure that the change will come about in a desired result. Similarly, their opposition to the proposed change may lead to a breakdown or complete failure of the process.

Commitment Planning: Critical Mass Evaluation

Critical mass may be determined for any such organizational change process, in

part, by reviewing the key stakeholders in the key stakeholder analysis accomplished during the SWOT process. Each organization and each issue under consideration will present unique critical mass components. In considering a critical mass evaluation, it is also a good idea to seek input from others to make sure that none of the key individuals or groups have been inadvertently left out of the process. Doing so could potentially impact the desired outcome. The stakeholders and snaildarters identified in the strategic planning process were one source for consideration as the critical mass. These are:

- Chancellor of the statewide university system
- President of the university
- University president's cabinet (chief of staff, provost, vice president's)
- University police chief
- University police department command staff, supervisors, and officers
- University security system analyst
- University chief information officer and his staff of information technology employees

Critical Mass Commitment

The commitment chart displayed in table 4.1 identifies the nature of current positions and desired positions of those individuals and groups who constitute the critical mass for the issue of implementing a biometric technology system for site security at CSU Monterey Bay. Those who have already bought into the change can assist in moving individuals or groups to desired positions through a concerted effort. Typically, this group is made up of the organization's management team, as well as other key stakeholders who have adopted the change as the collective vision of their own.

The critical mass commitment chart is presented in Table 4.1.

CRITICAL MASS COMMITMENT FOR BIOMETRIC TECHNOLOGY IMPLEMENTATION				
Critical Mass Members	Block Change	Let Change Happen	Help Change Happen	Make Change Happen
Chancellor of university system			X→	O
University President			X→	O
University President's cabinet			X→	O
University police chief			X→	O
UPD staff		X→	O	
University security systems analyst			X→	O
University CIO and staff			X→	O

Table 4.1

Analysis of the critical mass provides leaders with an overall picture of the present positions of key groups and individuals in the transition process. The present state is symbolized with an “X” and the ideal state is symbolized with an “O”. The arrow indicates the desired path for a successful transition.

Transition Management Structure

The police chief of a university law enforcement organization, in his or her role as the leader of the organization, is in the best position to promote vision, inspire others, and impart enthusiasm for any public safety organizational change. Regardless if the vision was the chief's idea, he or she is recognized as the leader of the organization. As such, he or she has position power within the organization and should take the lead as the transition manager for any significant organizational transition into biometric technology for site security in a university setting. What the designation of transition manager says is that the chief is 100 percent behind the transition and is confident the organization is

moving in the right direction. It will also position them to liaison with the university policy makers on important matters related to policy direction, budget, and other issues of concern regarding the organizational change.

The university police chief will liaison with a designated project manager who will keep him/her informed on all matters of importance regarding the change process. Depending on the complexity of the transition, it may also be prudent to form a transition team. This team should be made up of key management staff and others who have an interest in seeing the transition through to fruition. This team may be useful to accomplish some of the heavy work associated with a complex transition, such as budgetary issues or other tasks that may require some degree of administrative expertise.

Techniques and Methods of Implementation

Successfully persuading members of the critical mass constituency to move from their original position to the desired position is oftentimes critical to the success of the transition. The best way to accomplish this is through stakeholder participation, education and communication. This process at times can seem redundant, time consuming and even unnecessary, although it is critical to the success of successful implementation. Sharing information is perhaps one of the single most important things a leader can do when implementing organizational change. Sharing information in this process results in removing the mystique of uncertainty from the change process and it allows others to break the barrier of fear from the unknown. This communication and educational process should be part of any significant organizational transition. The process may take many forms including university public forums, department meetings, newsletters, and any other medium that will help get important information out. In some instances, it may be

necessary to make individual presentations to certain key individuals and/or groups to positively promote the transition. This will aid to set their minds at ease and these actions may even result in negotiations regarding certain matters pertaining to the transition.

Responsibility Charting

Responsibility charting lists the stages needed to initiate changes during the transition to a biometric technology system for site security. The chart outlines role responsibilities to accomplish the strategic plan. Responsibility charting reduces conflict between the stakeholders because roles are clearly defined and understood. The responsibility chart for the transition to a biometric technology system for site security is described in Table 4.2. This responsibility chart is similar for each phase of an incremental plan and will assist when assessing the impact of implementing biometric technology for site security into the organization.

RESPONSIBILITY CHART							
DECISIONS	PARTICIPANTS						
	Chief	Project Manager Police Lt	Police Sgt's	Police Officers	CIO/ Staff	Admin Analyst	Finance Director
Set Initial Planning Meeting	S	R	S	S	S	S	S
Select Advisory Committee	S/I	R	S	S	S	S	S
Select Committee Chairpersons	S/I	R	S		S		
Establish Goals & Objectives	S/I	R	S	S	S	S	S
Develop Policy Guidelines	S/I	R	S	I	I	S	S
Resource ID & Commitment	S/I	R/A	A	I	I	S	S
Develop Evaluation Components	S/I	R	S	I	I		
Set Implementation Dates	S	R	S		S	S	S
Conduct Training	S	S/I	R	I	S/I	S	S
R = Responsibility (not necessarily authority) A = Approval (right to vote) BLANK = No role				S = Support (put resources toward) I = Inform (to be consulted before action)			

Table 4.2

The responsibility chart is similar for each phase of an incremental plan and will assist when assessing the impact of implementing biometric technology for site security into the organization. The responsibility chart implies the accomplishment of several objectives toward the goal of implementing biometric technology for site security at CSUMB. The university police chief provides executive management oversight to the project manager, who is a police lieutenant and second in command of the organization. An initial planning meeting will occur and advisory committees and committee chairpersons will be identified. The committees will then establish goals and objectives and develop policy guidelines. Resource identification and commitment, evaluation development components, setting implementation dates and conducting training is additionally included in the responsibility chart.

Evaluation

A key component of this organizational change or implementation of new technology within any organization is to gauge the success of the change by developing evaluation components. The project manager has the responsibility of monitoring the success of the project and reporting issues, positive and negative, to the police chief. This could occur informally on a regular basis and more formally by completing a monthly status report. Once implemented, the evaluation of this technology and its impact on site security at CSUMB could be measured in several ways. Two examples are:

- Crime statistics on campus should be closely monitored to determine if the implementation of this technology for site security is having an impact on the crime rate.
- A customer satisfaction survey of faculty, staff, students and those employees directly involved in the operation of the biometric site security system can determine if they are satisfied with the system and to determine if any modifications need to be made.

The organization needs to be flexible and prepare to modify the operation of the site security system if crime statistics, customer input or employees operating the system indicate modifications need to be made that allows the system to operate more efficiently.

The transition to biometric technology for site security is a huge undertaking to the organization and its leaders. It is worth repeating that change is naturally resisted and the process is risky organizationally. It is also worth noting that during any period of change and uncertainty, there is tremendous opportunity. The hope for a better future for site security exists with biometric technology and its benefits outweigh the risks.

Recommendations for the successful implementation of a biometric technology site security system in a small university are examined in the next chapter.

CHAPTER V

RECOMMENDATIONS AND CONCLUSIONS

Recommendations

Biometric technology for site security will play a part in the future of university law enforcement. By 2009, it is anticipated that biometric technology for site security will be popular on college campuses. Today, biometrics is gaining popularity in physical security at a variety of public and private facilities.²⁴ This technology could be used in the future to control access to secure locations such as dormitories, classrooms, and a variety of other rooms or buildings in a university setting. Unlike photo identification cards for entry into certain buildings, which must be verified by someone monitoring a fixed post, biometrics permit unstaffed access control. Biometric devices, typically hand geometry readers, are becoming popular for access control in office buildings, hospitals, casinos and health clubs.²⁵ Biometrics can also be useful for high-volume access control, such as a university environment. For example, biometrics controlled access of 65,000 people during the 2000 Olympic Games, and Disney World in Florida uses a biometric fingerprint scanner to verify season-pass holders entering the theme park.²⁶

For those advocating the widespread use of biometrics, there appears to be numerous advantages to doing so. Biometric supporters say biometrics increases privacy rather than invading it. According to A. Etzioni in his 2001 book titled, *The Limits of Privacy*, biometrics will reduce identity fraud because thieves won't be able to steal personal data and assume that persons identity. He goes on to say biometrics will enhance privacy by ensuring individuals are who they claim to be.²⁷ Many see biometrics as a quality of life enhancement for society as a whole.

The Leadership Factor

Leadership is critical to both a successful strategic plan, as well as a transitional management plan. In any change process, leaders are key. In their book, *The Leadership Challenge*, authors Kouzes and Posner said it well, “Beyond the horizon of time is a changed world, very different from today’s world. Some people see beyond that horizon and into the future. They believe that dreams can become a reality. They open their eyes and lift our spirits. They build trust and strengthen our relationships. They stand firm against the winds of resistance and give us the courage to continue the quest. We call these people leaders.”²⁸

The following are general recommendations for university law enforcement leaders who are contemplating the implementation of hand reader biometric technology site security system to enhance the safety and security of buildings on their campus, to advance operational efficiency and effectiveness and to improve the overall feeling of safety for those who study, live, or work in a university setting. In general, the recommendations are relevant to many areas of strategic planning and organizational development. They also happen to be significant desirable leadership characteristics and capabilities.

- Leaders should utilize strategic planning and transitional management to affect change and accomplish organizational goals.
- Leaders should thoroughly understand the proposed change itself (i.e. biometric technology for site security). “What things will help us do better?” “What will we be able to do that we do not do now?” “What are the possible pitfalls and unforeseen consequences?”
- Leaders should ensure that the proposed organizational change is congruent with the campus community’s needs and desires.

- Leaders should work collaboratively with others in law enforcement to improve the integration of technology into policing.

Conclusions

When assessing how the implementation of biometric technology for site security will impact a small university police department by 2009, the future of biometric technology for site security in university policing seems almost a certainty. In many ways, it is a natural extension of those universities that currently have proximity card readers for building and site security; biometric technology will take site security to the next level. But to take full advantage of this emerging technology, it will require more than just the technological know-how and the financial resources. It will also require a greater degree of collaboration and partnership between law enforcement organizations and the communities they serve.

The recommended strategies in this paper are based on literature research, interviews with biometric technology innovators, security consultants and a campus community cross-section panel. The implementation of biometric technology for site security in a university setting will require a paradigm shift at every level of the organization; this will be the greatest impact and challenge. But the implementation of this technology, if approached correctly, has the potential to bring the campus community closer together and more involved with its university police department.

The impact of implementing biometric technology for site security at a university could be tremendous as many factions both internal and external to the organization may have fundamental opposition to its implementation. The successful integration of this emerging technology into university policing will truly require a law enforcement leader

with a futures mindset; and one who has vision, communication, leadership and organizational skills.

The primary focus of this research project has been to answer the issue question: How will biometric technology impact site security in a small university police department by 2009? The research revealed that various forms of biometric technology are becoming popular outside of law enforcement. Casinos, state welfare systems, airport security, airline ticketing and border control have cut costs by having biometric technology perform the work of many employees.²⁹ The technology is even being used as a replacement to the traditional time clock at job sites to ensure that employees are not clocking in or out for other employees.³⁰

While several forms of biometric technology, including iris scanning devices, hand geometry devices, facial recognition and voice recognition were discussed prior in this paper, it is suggested that hand geometry be the likely choice to be utilized for the purpose of site security in a university environment. The primary focus with implementing this technology on the CSUMB campus should be site security in the residential halls and classrooms.

There are many benefits to implementing this technology for site security at a university, which include: enhanced safety and security for students, faculty and staff; quality of life issues; the technology would increase privacy rather than invading it. Some of the challenges to implementing this technology include: social and political opposition to the use of this technology and technological and economic constraints.

Recommendations for the future

Biometric technology can enhance site security at CSU Monterey Bay and other university campuses nationwide. In planning for a future change to biometric technology for site security in a university setting, the following steps should be taken into consideration:

- Identify core strategies for achieving the goal.
- Develop a set of quantifiable measures for success.
- Develop a set of alternatives that allow for flexibility if some change strategies don't work.
- Adhere to an implementation plan that sets timelines and accountability for roles and responsibilities.
- Ensure that proper funding sources are allocated for the system acquisition. This includes seeking outside funding sources.
- Develop recognition and reward systems that honor those committed to the change.
- Communicate the plan so that everyone in the organization understands the direction, process, need, benefit and desired outcome of the change.
- Conduct regular meetings with key personnel involved in the change for progress reports and suggested implementation improvements.

In the final analysis, if either the campus community or the organization would feel better if biometric technology for site security was not in place, then it should not be utilized, despite its clear advantages.

APPENDIX A

NOMINAL GROUP TECHNIQUE

Ms. Michelle Donohue
Associate Director of Residential Life
CSU Monterey Bay

Mr. Troy Holt
Transportation and Parking Services Administrator
CSU Monterey Bay

Mr. Earl Lawson
Detective Sergeant
CSU Monterey Bay

Mr. Jay McTaggart
Police Lieutenant
CSU Monterey Bay

Ms. Lisa Moreno
Associated Student Body President
CSU Monterey Bay

Mr. Ron Smith
Associate Director of Information and Network Services
CSU Monterey Bay

Mr. Tim Riggs
Supervisor, Security Systems Services and Lockshop
CSU Monterey Bay

Mr. Richard Taylor
Director of Business and Support Services, Risk Manager
CSU Monterey Bay

APPENDIX B

POTENTIAL TRENDS IDENTIFIED BY NGT PANEL

1. Level of security measures
2. Obligation of the university to provide a safe environment
3. Level of convenience provided by biometric technology
4. Level of identity theft
5. Cost of technology
6. Acceptance of intrusiveness of advanced technology
7. Interconnectivity of various databases
8. Speed of technology and its obsolescence
9. Level of standardization with biometric technology
10. Disgruntled employee sabotages IT system database
11. Terrorist suicide bombers
12. Public awareness of how biometric technology can be used
13. Sophistication of biometric technology
14. Collection of citizen data for biometric database
15. Reliance of technology by a government agency
16. Development of new technology
17. Change in workforce
18. Development of new identity data bases
19. Terrorism and public safety concerns
20. Public concerns of personnel cost

First nine trends were the top selected trends by the NGT panel

APPENDIX C

POTENTIAL EVENTS IDENTIFIED BY NGT PANEL

1. Terrorist attacks on educational institutions nationwide
2. Legislation passes regarding implementation of biometric technology
3. Computer network virus infects CSUMB information technology database
4. Serial rapist selects CSUMB to commit crime
5. California State University system standardizes site security systems
6. Significant identity theft on campus
7. Police misuse biometric technology database information
8. Computer database system containing biometric data crashes
9. Mentally deranged suspect's actions thwarted with biometric technology
10. students commit vandalism to biometric technology equipment
11. Homeland security grant funding increased for purchase of equipment
12. University police solves sex crime after reviewing database on who entered a building at a specific date/time
13. Female students demand biometric technology be installed in female only residential hall

First nine events were the top selected events by NGT panel

ENDNOTES

- ¹ Curt Blakeney, "Can Biometrics Save the World?" Newsweek Magazine, October 2003
- ² State of California, The Commission on Peace Officer Standards and Training Administrative Manual, May 2003
- ³ A. Jain, "Biometrics: Personal Identification in a Networked Society." Kjlwre Academic Publishers, 1999.
- ⁴ Kellie Speed, "Biometrics Gain Momentum", Security Magazine. March 2003, 44-45.
- ⁵ Bill Spence, "How is Biometrics Integrated Into Access Control Applications?" Public Venue Security Magazine website, 2003; available from <http://www.publicvenuesecurity.com>; internet accessed July 7, 2004
- ⁶ S. Lui and M. Silverman, "A Practical Guide to Biometric Security Technology", IEEE Computer Society Magazine, January 2001.
- ⁷ Joseph Campbell, "Government Applications and Operations", Biometric Consortium website, 2004; available from <http://www.biometrics.org>; internet accessed June 21, 2004
- ⁸ *ibid.*
- ⁹ Michael Sasso, "New Time Clocks Keep Employees Honest." The online ledger website, 2004; available from <http://www.business@theledger.com>; internet accessed May 21, 2004
- ¹⁰ *ibid.*
- ¹¹ *ibid.*
- ¹² Charles Hill and Gareth Jones, "Strategic Management: An Integrated Approach", 4th ed., (Boston: Houghton Mifflin Company, 1998).
- ¹³ P. Prabhakar, "Biometric Recognition: Security and Privacy Concerns", IEEE Security and Privacy Magazine, Vol. 1, No.2, pp-33-42, March 2003 edition.
- ¹⁴ *ibid.*
- ¹⁵ John Taschek, "An Eye on Biometrics." Available from <http://www.eweek.com>; internet accessed May 28, 2004.
- ¹⁶ Gail R. Light, "Security vs Liberty: Weighing the Options." MSU Today; available from <http://biometrics.cse.mse.edu>; internet accessed June 16, 2004
- ¹⁷ *ibid.*
- ¹⁸ CSU Master Plan, available from http://cpd.csUMB.edu/master_plan_index.html; internet accessed July 5, 2004.
- ¹⁹ CSU Monterey Bay annual crime statistics report, available from <http://police.csUMB.edu>; internet accessed May 5, 2004
- ²⁰ Security on Campus web site, available from www.securityoncampus.org; internet accessed May 17, 2004.
- ²¹ Andre Delbecq; Andrew Van de Ven and D. Gustafson, "Group Techniques for Program Planning: A Guide to Nominal Group and Dephi Processes". Green Briar Press, Middleton, WI, 1986.
- ²² *ibid.*
- ²³ *ibid.*
- ²⁴ Sharon Begley, "What Price for Security?" Newsweek Magazine, (October 2003).

²⁵ “Hand Geometry Preferred Biometric in 45% of All Control Applications”, available from <http://www.handreader.com/news>; internet accessed January 7, 2004.

²⁶ *ibid.*

²⁷ A. Etzioni, “Big Brother or Big Benefits? The Limits of Privacy.” New York: Basic Books, 1999.

²⁸ James Kouzes and Barry Posner, “The Leadership Challenge.” Jossey-Bass Publishers, San Francisco, 1995.

²⁹ *ibid*

³⁰ *ibid*

BIBLIOGRAPHY

- Begley, Sharon. "What Price Security?" *Newsweek*, (October, 2003).
- Blakeney, Curt. Can Biometrics Save the World? Public Venue Security Magazine website, 2003; available from <http://www.publicvenuesecurity.com>; internet accessed 7 July 2004.
- Blakeney, Curt. Super Bowl, Super Security. Public Venue Security Magazine, November/December 2003, 12-13.
- Brin, David. *Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Addison-Wesley Press, New York, NY, 1998.
- Campbell, Joseph. Government Applications and Operations. Biometric Consortium
- Coleman, Stephen Ph.D. Solving Cases of Mistaken Identity and More With Biometrics. The Journal. Fall 2002. Computer World.
- D'Agostino, Salvatore. Leveraging the Infrastructure, Seeking the Holy Grail of Building Systems. Buildings Magazine, July 2004, 36.
- Delbecq, Andre; Andrew Van de Ven and D. Gustafson. *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*. Green Briar Press, Middleton, WI, 1986.
- Etzioni, A. "Big Brother or Big Benefits? The Limits of Privacy. New York: Basic Books, 1999.
- Hill, Charles W. and Gareth Jones. *Strategic Management: An Integrated Approach*, 4th ed. Houghton Mifflin Company, Boston, 1998, 5.
- Jain, A. "Biometrics: Personal Identification in Networked Society". Kluwer Academic Publishers, 1999.
- Kouzes, James and Barry Posner. *The Leadership Challenge*. Jossey-Bass Publishers, San Francisco, 1995, 88-94.
- Light, Gail R. Security vs Liberty: Weighing the Options. MSU Today; available from <http://biometrics.cse.mse.edu>; internet accessed 16 Jun 2004
- Lui, S. and Silverman M., "A Practical Guide to Biometric Security Technology", IEEE Computer Society IT Pro-Security (January 2001), 27-32.

Prabhakar, P. Biometric Recognition: Security and Privacy Concerns, IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp 33-42, March 2003 edition.

Sasso, Michael. New Time Clocks Keep Employees Honest. They Are Activated Only by One's Hand. The online ledger website, 2004; available from <http://www.business@theledger.com>; internet accessed 7 Jan 2004

Speed, Kellie. Biometrics Gain Momentum. Security Magazine, March 2003, 44-45.

Spence, Bill. How is Biometrics Integrated Into Access Control Applications? Public Venue Security Magazine website, 2003; available from <http://www.publicvenuesecurity.com>; internet accessed 7 July 2004.

Taschek, John. An Eye on Biometrics. Available from <http://www.eweek.com>; internet accessed 30 Jun 2004.