Crime Analysis

for Problem Solving Security Professionals
in 25 Small Steps

Karim H. Vellani, CPP, CSC

KARIM H. VELLANI

Karim H. Vellani is an independent security consultant at Threat Analysis Group, LLC, a security consulting firm and Past President of the International Association of Professional Security Consultants. Karim is Board Certified in Security Management (CPP), a Board Certified Security Consultant (CSC), has over 15 years of security management and forensic security consulting experience, and has a Master's Degree in Criminal Justice Management. He is the author of two books, Applied Crime Analysis and Strategic Security Management, and has contributed to a number of other security related books and journals.

Karim developed a crime analysis methodology that utilizes the Federal Bureau of Investigation's (FBI) Uniform Crime Report coding system and a proprietary software application called CrimeAnalysis™. Karim has also developed a Risk Assessment Methodology for Healthcare Facilities and Hospitals. In 2009, the International Association of Healthcare Security and Safety (IAHSS) published its *Security Risk Assessment* Guideline, which was authored by Karim at the request of IAHSS.

As an Adjunct Professor at the University of Houston - Downtown, Karim taught graduate courses in Security Management and Risk Analysis for the College of Criminal Justice's Security Management Program. Annually, Karim instructs for the International Association of Professional Security Consultants and ASIS-International.

Karim may be contacted at (281) 494-1515 or via email at kv@threatanalysis.com.

Contents

EXECUTIVE SUMMARY

While the daily assessment of terror threats applies primarily to security professionals who are charged with protecting critical infrastructure assets, such as chemical plants, oil refineries, and transportation ports, most security professionals focus on terrorism as a high risk, low probability concern which needs to be addressed on an irregular basis. Once terrorism contingency plans, emergency procedures, and business continuity plans are established, security professionals can once again turn their attention to the daily risks that threaten an organization's assets. Everyday crimes are the most common threat facing security professionals in protecting their assets (targets) and a thorough assessment of the specific nature of crime can reveal possible weaknesses in a facility's security posture and provide a guide to effective solutions. A full understanding of everyday crime at specific sites allows security professionals to select and implement appropriate countermeasures to reduce the opportunity for such incidents to occur again. Eck, Clarke and Guerette state that the greatest preventive benefits will result from focusing resources high risk sites ("risky facilities") because crime is heavily concentrated on particular people, places and things; that is for any group of similar facilities, a small proportion will experience the majority of the crime (Eck J. E., 2007).

Understanding crime has the primary benefit of assisting in good security decisions, which are effective in preventing real risks in a cost effective manner. Nick Tilley argues in favor of *analysis **for** crime prevention* as a driver for formulating prevention strategies. Analysis, according to Tilley, identifies concentrations of crime where there is a potential yield from prevention efforts and that analysis can help forecast future crime problems with the hope of developing preemptive strategies. More importantly, Tilley argues that analysis "helps find the most efficient, effective, and perhaps equitable means of prevention," what the industry might call optimization (Tilley, 2002).

Security optimization, sometimes referred to as data driven security, refers to using metrics or data to drive a security program and reduce risk. While not all elements of a security program lend themselves to measurement, many factors can be measured effectively. In larger organizations, the security department is a business unit, not unlike other business units within an organization that must justify its existence. Security, notes Gill, *needs to be businesslike and show how it contributes to the financial well-being of all aspects of organizational life* (Martin Gill, 2007). A key method for justifying security is to measurably reduce risk with an optimized security program.

Optimization is a concept utilized by organizations operating in dynamic environments to effectively manage risk. Security professionals face the unique challenge of providing security that reduces crime and loss, is cost effective, and does

not expose their organizations to undue liability. Thus, they must not only be knowledgeable about security technologies, but also good business decision makers and risk managers. Security costs should be commensurate with the risk and provide a measurable return on investment.

This Report, then, will answer the question: How does one measure the effectiveness of a *site specific* security program via crime analysis? More specifically, how do security professionals provide the optimal level of security for a site that not only reduces risk, but is also cost effective?

This Report is applicable to a broad spectrum of security professionals, including security professionals, facility managers, risk managers, and property managers. Ideally, readers will use the information to optimize their security programs. While the audience for this report is broad, facilities that serve the general public, such as retail stores, banks, hotels, gas stations, and the like will have a discernable benefit.

READ THIS FIRST

The purpose of this Report is not to identify the myriad threats that face an organization, nor to discuss the many components of a threat assessment. There are many books and articles that provide high level overviews of those topics. Instead, the purpose of this Report is to identify current research in security and crime prevention and identify the means of optimizing a security program of specific sites through informed decision making; that is through crime analysis. How does one measure the effectiveness of a site specific security program via crime analysis? More specifically, how do security professionals provide the optimal level of security for a site that not only reduces risk, but is also cost effective? And why focus on the micro rather than the macro? Why should security professionals hone in on site specific problems rather than problems that span the organization's facilities? Eck, Clarke and Guerette argue that the greatest preventive benefits will result from focusing resources high risk sites ("risky facilities") because crime is heavily concentrated on particular people, places and things; that is for any group of similar facilities, a small proportion will experience the majority of the crime (Eck J. E., 2007). Eck et al describe three implications that result from their research on risky facilities:

1. It is productive to divide places by facility type and focus prevention on homogeneous sets of facilities (e.g. banks, grocery stores, motels, etc.)

2. Focusing on the most troublesome facilities will have greater payoff than spreading prevention across all facilities, most of which have little or no crime

3. Any prevention measure will have to involve the people who own and run the facilities (e.g. property manager, branch manager, facilities director, etc.)
   (Eck J. E., 2007)

PREPARE YOURSELF

1. Learn the POP way

Problem-Oriented Policing (POP) serves as a model for security practitioners. According to Herman Goldstein, an early founder of the POP approach, "problem-oriented policing is an approach to policing in which discrete pieces of police business (each consisting of a cluster of similar incidents, whether crime or acts of disorder, that the police are expected to handle) are subject to microscopic examination (drawing on the especially honed skills of crime analysts and the accumulated experience of operating field personnel) in hopes that what is freshly learned about each problem will lead to discovering a new and more effective strategy for dealing with it" (Goldstein, 2009). Security practitioners can use a similar approach to addressing site specific problems through crime analysis.

Unfortunately, very little research has been conducted into crime analysis as it applies to the private sector. In fact, one could count on one hand the number of authors who have contributed to the private sector body of work. This gap has caused many businesses and organizations to rely heavily on information and studies generated by security service companies that service the end user organizations. The good news is that there has been a significant amount of research in and for the public sector, some of which is directly applicable to private sector business. We, the security industry, can turn to that body of knowledge to adapt it to sound security practices.

2. Meet Sherlock Holmes and his successors

To quote James Lipton, *we begin at the beginning*. Why is crime analysis important for security professionals? Sir Arthur Conan Doyle in his Sherlock Holmes mystery, A Study in Scarlet, said, "There is a strong family resemblance about misdeeds, and if you have all the details of a thousand at your finger ends, it is odd if you can't unravel the thousand and first." It is on that basic premise that crime analysis is based. "Crimes are patterned; decisions to commit crimes are patterned; and the process of committing a crime is patterned." (Brantingham, 1993). A crime pattern is a group of crimes that share common characteristics but are not necessarily attributed to a particular criminal or group of criminals. Understanding crime patterns, in time, in space, of target, can drive better security decisions. Better decisions help optimize a security program. Criminologist Nick Tilley argues in favor of *analysis **for** crime prevention* as a driver for formulating prevention strategies. Analysis, according to Tilley, identifies concentrations of crime where there is a potential yield from prevention efforts and that analysis can help forecast future crime problems with the hope of developing preemptive strategies. More

importantly, Tilley argues that analysis "helps find the most efficient, effective, and perhaps equitable means of prevention," what we might call optimization (Tilley, 2002). Optimization is as *an act, process, or methodology of making something (as a design, system, or decision) as fully perfect, functional, or effective as possible; specifically the mathematical procedures (as finding the maximum of a function) involved in this*. (Merriam Webster, 2009).

3. Grasp the theories

The following discussion provides a broad overview of the theoretical underpinnings of current security practices. Security professionals often function in dual roles, prevention and response: prevent what can be prevented and be ready to respond to what cannot be prevented. As such, there are three options for responding and adapting to emerging risk:

1. Eliminating or intercepting threats before they attack

2. Blocking vulnerabilities through enhanced security

3. Reducing the consequences after the incident occurs

Logically, the best approach for mitigating risk is a combination of all three elements, decreasing threats, blocking opportunities, and reducing consequences. By way of example, we can look at the Department of Homeland Security's efforts in the war on terror. The United States homeland security strategy may be characterized as the three P's: Prevent, Protect, and Prepare in that the Department of Homeland Security's strategy is to reduce the threat by way of cutting terror funding, destroying terrorist training camps, and capturing terrorists; to block opportunities through enhanced security measures such as increased airport and maritime security; and to reduce the consequences through target-hardening efforts which minimize damage such as window glazing and by shortening response and recovery times such as moving the Federal Emergency Management Agency under the Department of Homeland Security.

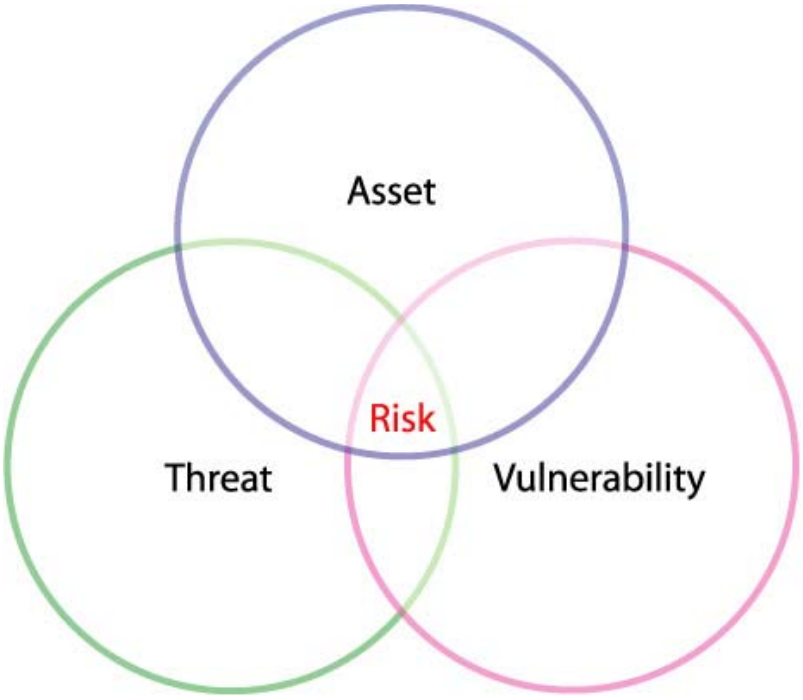
Environmental Criminology, which forms the foundation for much of what we do in the security field, emphasizes the importance of geographic location and architectural features as they are associated with the prevalence of criminal victimization. According to this school of thought, "crime happens when four things come together: a law, an offender, a victim or target, and a place. Environmental criminologists examine the fourth element -- place (and the time when the crime happened). They are interested in land usage, traffic patterns and street design, and the daily activities and movements of victims and offenders" (School of Criminal Justice at Rutgers University, 2009).

4. Know the recipe for risk

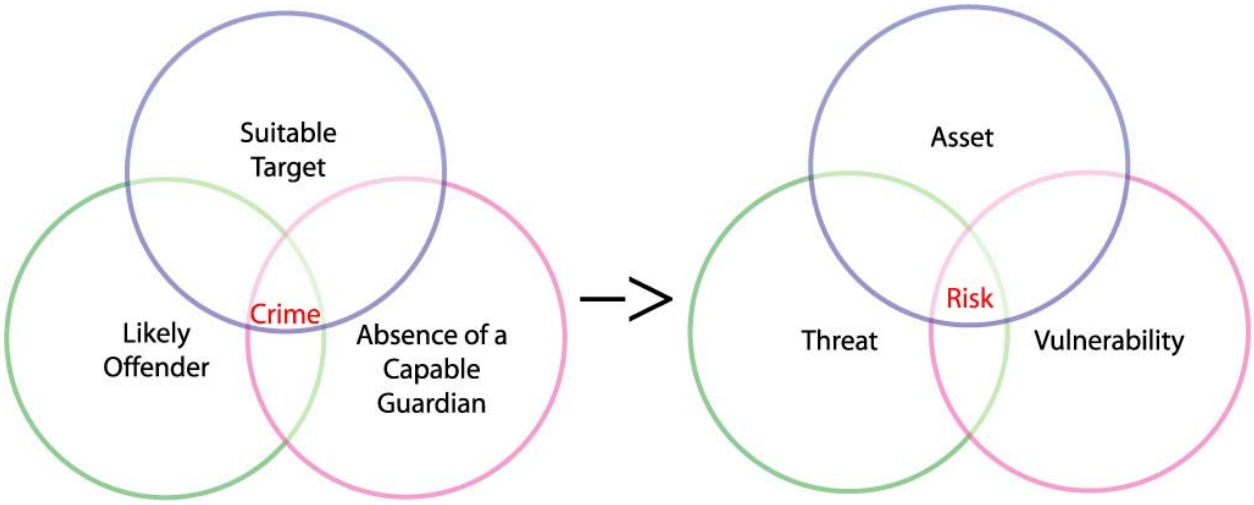
Noted environmental criminologist Marcus Felson states that criminal acts almost always have three elements:

1. a likely offender
2. a suitable target
3. the absence of a capable guardian against the offense (Felson, 2002)

In the field of security, reducing risk is a key goal. Risk is defined as *the possibility of asset loss, damage, or destruction as a result of a threat exploiting a specific vulnerability* (Vellani, 2006) or alternatively as *the possibility of loss resulting from a threat, security incident, or event* (ASIS-International Guidelines Commission, 2003). As illustrated below, risk exists at the intersection of assets, threats, and vulnerabilities.



When seen together, the two concepts illustrate the similarities between theory and practice:



In practice, risk managers typically utilize five strategies for mitigating risk. These strategies include avoidance, reduction, spreading, transfer and acceptance. Security is generally concerned with risk reduction, wherein security professionals are charged with reducing organizational risk by providing sufficient protection for assets. One tactic for reducing risk is to reduce the opportunity for security breaches to occur.

5. Understand the crime triangle

The effectiveness of risk reduction is based on the concept of the *crime triangle*, shown below, which identifies the necessary elements for crime to occur.

All three elements, motive, desire, and opportunity, must exist for a crime to occur. Capability and motive are characteristics of the criminal perpetrator. Opportunity, on the other hand, is a characteristic of the asset, or more specifically around the asset (target of crime). In the security professional, the term *opportunity* is used interchangeably with the term *vulnerability*. Eliminating or reducing opportunities (vulnerabilities) is a primary goal of most security programs. If opportunities are eliminated, crime does not occur, as illustrated below.

6. Change the situation

Once the nature of crime is known, environmental criminology tells us that there are many techniques for reaching the goal of reducing and/or eliminating opportunities. A quick scan of *Situational Crime Prevention's* techniques for preventing crime also shows remarkable similarities between theory and security practices:

Twenty-Five Techniques of Situational Crime Prevention (Clarke, 2005)

Increase the Effort	1. Harden Targets
	2. Control access to facilities
	3. Screen exits
	4. Deflect offenders
	5. Control tools/weapons
Increase the Risks	6. Extend guardianship
	7. Assist natural surveillance
	8. Reduce anonymity
	9. Utilize place managers
	10. Strengthen formal surveillance
Reduce the Rewards	11. Conceal targets
	12. Remove targets
	13. Identify property
	14. Disrupt markets
	15. Deny benefits
Reduce Provocations	16. Reduce frustration and stress
	17. Avoid disputes
	18. Reduce emotional arousal
	19. Neutralize peer pressure
	20. Discourage imitation
Remove the Excuses	21. Set rules
	22. Post instructions
	23. Alert conscience
	24. Assist compliance
	25. Control drugs /alcohol

THE BUSINESS OF SECURITY

7. Know that business comes first

The phrase "it's the economy, stupid," coined by former President Clinton's campaign strategist, refers to the simple and singular message of a successful political campaign. It's equally applicable to a successful security program. Economics is a significant driver of security, both in terms of pushing dollars to reduce loss as well as pulling dollars away to cut costs and protect the bottom line. Making the business case for security is an increasingly critical function of security professionals. In larger organizations, the security department is a business unit, not unlike other business units within an organization that must justify its existence. A key method for justifying the department is to optimize security such that risk is measurably reduced, and security costs are manageable.

Optimization is a concept utilized by organizations operating in dynamic environments to effectively manage risk. Security professionals face the unique challenge of providing security that reduces crime and loss, is cost effective, and does not expose their organizations to undue liability. Success can be achieved through a carefully orchestrated balancing act of three tasks:

1. Monitoring risk in real time or near real-time

2. Deploying effective security measures which reduce risk

3. Working within reasonable financial limitations

Optimizing security is an effective method for balancing these tasks. In order to be successful at this balancing act, security professionals must not only be knowledgeable about security technologies, they must also be good business decision makers and risk managers. Security costs should not exceed reasonable budgets and preferably, provide a measurable return on investment. The security program should also effectively reduce risks to an acceptable and manageable level.

Optimization can ensure that security professionals are successful in all three of the factors outlined. How can security professionals justify a sizable and increasing security budget to senior management? By now, most security professionals are keenly aware that a security program's success depends on the commitment and support, or buy-in from senior executives. Using anecdotal evidence to justify spending on physical security measures and costly protection personnel no longer suffices.

A security program driven by data and metrics helps drives decisions. "It replaces intuition with hard data" (Jopeck, 2000). Data and metrics justifies expenses to senior management by showing the proof of success that can garner that necessary buy-in and demonstrate a convincing return on investment. Specifically, metrics guide decision making in the following areas:

- allocation of resources (money and staff);
- consideration of new technologies;
- identifying risks faced by the company; and
- implementing methods of mitigating those risks (Cavanagh, 2008).

8. Don't feed the lawyers

Before discussing legal standards, it might be appropriate to include a disclaimer: The author is not providing legal advice and legal counsel should be consulted on these issues. With that said, two legal factors should be considered when optimizing security: *Expert Testimony* and *Foreseeability of Crime*. These factors should be considered because of the impact that negligent security litigation may have on the organization, directly and indirectly. Decisions that are made in the board room (or at least in the security conference room) may be tested during the litigation process. The validity of a security methodology or risk model will be scrutinized. Individual components that make up the broader methodology will be evaluated. Unfortunately, unless one is actively involved in the litigation process or debriefed by defense counsel, few lessons are learned that can then be applied to security decisions in the future.

The first factor is expert testimony. Expert testimony is often used when an organization is sued for negligent or inadequate security. When necessary, the defense and/or the plaintiff's attorney retain a security expert to explain to the judge and jury what level of security is required at the property, if any, based on the risk to the organization and its assets (people, property, and information).

Experts, by definition, must rely on a sound and reliable methodology such as the one described in this report. More frequently, experts are used to determine if the defendant organization's decision making process was sound. An organization that uses an unreliable methodology may suffer from criticism from an expert, even one that was retained by their defense counsel. Similarly, using an unreliable methodology is problematic for the primary reason that the court will not allow unreliable evidence in court. Some crime analysis methodologies are sound, while others are not.

The rule for expert testimony is rather simple: Experts cannot rely on junk science or unreliable methodologies. This rule was articulated in the U.S. Supreme Court case, *Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993)*. Experts are routinely subjected to *Daubert* Challenges wherein their opinions are challenged and possibly excluded from testifying on the case at hand. Commonly referred to as the *Daubert* Factors, the questions asked by the court include:

1. Can the relied upon theory/technique be tested and has it been tested?
2. Has it been subjected to peer-review and publication?
3. What is the known or potential error rate?
4. Is the theory/technique accepted within the relevant field?

For the security professional, *Daubert* begs two questions: Was the decision making process (methodology or risk model) and data that the defendant organization used to make decisions reliable. Is the data that the expert witness uses to demonstrate adequate security, or lack thereof, reliable. Reliability, according to the U.S. Supreme Court, is determined by a tested theory which has been subjected to peer-review and publication, has a known error rate, and is accepted within the security industry. Crime analysis is the one component of a threat assessment that can meet the challenge of *Daubert*.

The applicability of *Daubert* to individual states varies by state. Some states have accepted it in whole or in part, while others have modified it or developed their own tests for admissibility of expert testimony. *Daubert* suggests that security practitioners should evaluate their decision making practices in light of the *Daubert* factors. Specifically, can each element of their risk model or methodology individually withstand the scrutiny of a *Daubert* challenge? In the context of this paper, is the crime analysis methodology based on research or is it based on junk science?

The second legal factor that should be considered is the foreseeability of crime. A negligent security lawsuit is a civil action brought on behalf of a person seeking damages for negligent or inadequate security against the owners and their agents of the property where the injury or loss occurred. Generally, three elements must be met in order for a Plaintiff to prevail in a premises security lawsuit. These elements are: duty, breach of duty, and proximate cause. Duty is the element we'll focus on in this section as it directly relates to the metrics and data used by the defendant organization. Duty is determined by the foreseeability of crime:

1. Past episodes of the similar or related activities on the property

2. Similar crimes in the immediate vicinity (high crime area)

3. That the facility itself attracts crime (inherent threats)

"The element of *foreseeability* is essentially a question of whether the criminal act was one that a reasonable person would have foreseen or reasonably anticipated, given the risk of crime that existed at the time of the assault at the property in question. Ultimately whether a crime is considered legally *foreseeable* will depend on the court, the jury, and the laws of that state" (Bates, 2006).

While some states take a conservative approach to foreseeability by considering only *prior similar crimes*, other states are more liberal and look at the *totality of the circumstances*. Regardless of the state, all consider crimes on the property when determining whether or not the crime was foreseeable.

"The *prior similar crime* rule is the older, more conservative approach and requires that there be some evidence of prior crimes that are similar in nature to the one complained of in the plaintiff's case" (Bates, 2006). An example of this is a Texas Supreme Court case, *Timberwalk v. Cain*, which outlines the specific factors necessary for establishing foreseeability of crime in premises liability lawsuits. In *Timberwalk*, the court set forth five criteria for measuring the risk of crime including recency, proximity, publicity, frequency, and similarity of past crimes. Other states share the prior-similar test, such as California, New Mexico, Montana, and New York (Pastor, 2007).

The other commonly used foreseeability test is the *totality of the circumstances* rule. "Under this rule, evidence is typically allowed to show the existence of prior dissimilar crime, crime in the neighborhood, and other risk factors to determine whether a crime was foreseeable" (Bates, 2006). Many states follow this rule including Colorado, Georgia, Massachusetts, Nevada, New Jersey, and Ohio (Pastor, 2007).

9. Know your industry

In recent years, industry associations have promulgated guidelines which advise security professionals on the use of crime statistics and other threat data. Though the guidelines

presented below are not standards, they are developed using a rigorous process and approved by member consensus.

ASIS-International's *General Security Risk Assessment* guideline states that among the information sources for determining loss risk events are local police crime statistics. Specifically, the guideline identifies one source of crime-related events is "local police crime statistics and calls for service at the site and the immediate vicinity for a three-to-five year period" (ASIS-International Guidelines Commission, 2003)

The International Association of Professional Security Consultants' *Forensic Methodology* (Best Practice #2) states, "a comprehensive threat assessment considers actual, inherent, and potential threats" (International Association of Professional Security Consultants, 2008). The Forensic Methodology also defines actual, inherent, and potential threats:

1. *Actual Threats*
    a. *The crime history against an asset or at a facility where the asset is located. Actual threats are a quantitative element of a threat assessment.*

    b. *Relevant crimes on the premises (three to five years prior to the date of the incident)*

    c. *Relevant crimes in the immediate vicinity of the facility (three to five years prior to the date of the incident)*

2. *Inherent Threats -*
    Threats that exist by virtue of the inherent nature or characteristics of the facility or nature of the operation. For example, certain types of facilities or assets may be a crime magnet or prone to loss, damage or destruction (e.g., assaults among patrons in nightclubs, infant abductions from hospital nurseries, etc.).

3. *Potential Threats*
    Threats which exist by virtue of vulnerabilities around the asset or weaknesses in the security program which produce opportunities for crime to occur. (International Association of Professional Security Consultants, 2008)

While ASIS-International and the International Association of Professional Security Consultants directly serve the security industry, other associations have published guidelines that indirectly

support the need for crime analysis. For example, the Illuminating Engineering Society of North America's *Guideline for Security Lighting for People, Property, and Public Spaces* states, "the most reliable means of determining future security needs and criminal vulnerabilities is to conduct a crime analysis" (Illuminating Engineering Society of North America, 2003). The National Fire Protection Association's *Guide for Premises Security* states that when conducting a security vulnerability assessment, crime statistics should be considered (The National Fire Protection Association, 2005).

The on-going need to justify security expenditures and optimize security programs provides the reasoning for crime analysis. Industry guidelines also promote the use of crime analysis as part of an overall risk assessment. Further support is provided by case law as described above. Unfortunately, industry guidelines and case law don't provide much more than directives to conduct crime analysis. Industry practice in this regard varies across organizations and even within organizations. In other words, security professionals have not uniformly applied any single methodology in response to the crime analysis need, though calculating crime rates for a site or areas is prevalent. For guidance on the mechanics of crime analysis, environmental criminology and law enforcement related research and publications provide some help that can be applied to the private sector. Thus, the rest of this report will focus on the mechanics of conducting a useful crime analysis based on those sources and the few private sector sources that exist.

10. Know your competitors

Most companies engage in some form of data collection to document crimes, security breaches, and other relevant information. Other organizations prepare reports which summarize the data. Sophisticated organizations take the concept further and use the data to drive security decisions and optimize the program. The critical element for optimizing security is crime analysis and as such, the various methods used by industry today to analyze crime are presented in the rest of this report.

"Crime analysis is a key step in the sequence of activities aimed at conceiving, implementing and evaluating measures to prevent crime" (Ekblom, 1988). "Crime analysis rests on the assumption that crimes are not totally random, isolated and unique events, but can be combined into sets sharing common features and showing distinct patterns. It assumes crimes cluster in place and/or time, focus on particular types of property or victims and are committed by a particular range of methods" (Ekblom, 1988, Wortley, 2008). Certain facilities will have higher crime year after year, while others will experience lower crime and only isolated incidents. For each facility, however, other trends become evident, such as where and when

the crimes occur or the types of crimes that occur. One of the essential functions of crime analysis is to "identify the conditions that facilitate crime and incivility so that policymakers may make informed decisions about prevention approaches" (O'Shea, 2002). "Carrying out a crime analysis makes it possible to devise preventive measures appropriate to the local crime problem and its physical and social context" (Ekblom, 1988). "In general terms [local crime analysis] aims to address the following issues, regardless of the specific context in which the analysis is undertaken:

- to identify an area's crime problems through the analysis of data;
- to raise the level of awareness and understanding of the crime problems within an area; and
- to assist in the development of appropriate responses to those problems that are of concern" (Read, 1995).

Examining crimes perpetrated at company facilities is commonplace in today's business environment. In larger companies, there may be a person or group of people who are solely dedicated to the function of crime analysis usually working under the risk management or security departments. In smaller companies, the crime analysis function is carried by someone who also has other security management duties. Crime analysis may also be an outsourced function, whereby company personnel simply utilize crime data that a contractor has collected, entered into a database, and possibly provided some analytical work up or the tools to do so.

The second element is the analytical component. Crimes are analyzed in different ways depending on what one is trying to accomplish. Most commonly, facilities are ranked based on the crime level or rate. Generally, facilities with more crime or a higher crime rate are given a larger piece of the security budget, while less crime prone sites are given less security money. Crimes are also analyzed on a facility by facility basis allowing security professionals to select appropriate countermeasures.

Finally, crime analysis is used to assess and select appropriate countermeasures. Crimes that are perpetrated on a property can usually be prevented using security devices or personnel, however it should be noted that not all measures are cost-effective or reasonable. Certainly, a criminal perpetrator would be hard pressed to steal an automobile from a small parking lot patrolled by 20 security officers, though that type of security extreme is not reasonable, nor inexpensive. Crime analysis guides security professionals in the right direction by highlighting the types of crimes perpetrated (crime specific analysis), problem areas on the property (Hot spot analysis), and when they occur (temporal or time series analysis) among others. Using this information, it is much easier to select countermeasures aimed directly at the problem.

11. Ask the right questions

From a security perspective, crime analysis is defined as "the logical examination of crimes which have penetrated preventive measures, including the frequency of specific crimes, each incident's temporal details (time and day), and the risk posed to a property's inhabitants, as well as the application of revised security standards and preventive measures that, if adhered to and monitored, can be the panacea for a given crime dilemma" (Vellani, 2006). While this definition is multi-faceted, it can be dissected into three basic elements:

- The logical examination of crimes which have penetrated preventive measures
- The frequency of specific crimes, each incident's temporal details (time and day), and the risk posed to a property's inhabitants
- As well as the application of revised security standards and preventive measures

Alternatively, crime analysis may be defined as "the set of systematic, analytical processes that provide timely, pertinent information about crime patterns and crime-trend correlations" (Wortley, 2008). Understanding the factors that lead to crime and a comprehensive study of a property's crime helps optimize security by aiding in the selection of appropriate countermeasures and deployment schedules. A comprehensive crime analysis answers the four W and one H questions.

The *What* question tells us what specifically occurred. For example, was the crime against a person or property, violent or not, completed or attempted. *What* also distinguishes between types of crime that require different solutions such as whether a reported robbery was actually a burglary.

Where answers the location-specific question. Did the crime occur inside the walls of the location, in the parking lot, in the alley way behind the site? Did it occur in a public area or a secured area? Determining the precise location assists security professionals in creating additional lines of defense around targeted assets. For example, if the crime analysis indicates that a vast majority of loss at a small grocery store is occurring at the point of sale, then little will be accomplished by installing a lock on the back office where the safe is located. In this example, the crime analysis will rule out certain measures, but by the same token, crime analysis will also spotlight certain solutions, such as increased employee training or updated accounting systems at the point of sale.

The *When* question provides the temporal details. Knowing when crimes are most frequent helps in the deployment of resources, especially costly security measures such as personnel. Temporal details include the date, time of day, day of week, and season that a crime occurred. "The temporal distribution of crime is likely to be skewed, whether this be by time of day, day of the week or across seasons." (Read, 1995).

Who answers several important questions that help a security professional create an effective security program. Who is the victim(s) and who is the perpetrator? Knowledge of the types of criminals who operate on or near a given property assists security professionals in selecting the best measures to reduce crime opportunities. For example, gambling casinos have used Closed Circuit Television (CCTV) for some time to track known gambling crooks. Also important are the potential victims of crime. Ted Bundy and Jeffrey Dahmer, like other more common criminals, select particular types of victims. Thus, an understanding of the people that may be targeted focuses a security professional's attention. For example, a residential apartment complex that caters to recently released psychiatric patients has larger responsibility to provide a safe environment given the fact that their clientele are not usually capable of protecting themselves. The oldest example of the Who question dates back to premises liability law itself where innkeepers where often found to be responsible for the safety of a guest when crime was foreseeable. People on travel are usually not aware of the area in which they are staying and they also have little control over the security measures that they can take to protect themselves inside the hotel room.

How is the most consequential question to be answered by the crime analysis. How a crime is committed often directly answers the question *How* the crime can be prevented in the future. More specific *How* questions may also be asked. How did the criminal access the property? If we know that a criminal has accessed the property via a hole in the back fence of the property, efforts can be taken to immediately repair the fence. Other specific questions reveal the method of operation (MO). How did a criminal enter the employee entrance of an electronics store to steal a television? How did a burglar open the safe without using force? How did the car thief leave the gated premises without knowing the exit code? Obviously, the list of examples is unlimited and security professionals need to ask many questions about the criminal's actions as possible to learn the most effective solutions. It is true that often the *How* will be the most difficult question to answer. This leads into a problematic area as crime sources can be divided into two categories, internal and external. Internal sources of crime can be employees and other legitimate users of the space such as tenants. They are called legitimate users of the space as they have a perfectly valid reason for being at the location but in the course of their regular activities, they also carry out criminal activities.

Crime analysis provides the answers and arms security professionals to attack the crime problem. Security professionals have typically turned to three sources to understand threats

and optimize the security programs for their facilities: internal reporting systems, demographics, and crime data from law enforcement agencies. Internal reporting systems are simply formal or informal reporting mechanisms where employees and security personnel report crimes and other security incidents to centralized databases. The value of internal reporting systems is highly dependent on the type of system used and the consistency of data reporting from within the organization. Some employees will report every event that occurs, while others may report only certain incidents. To supplement internal reporting, most security professionals have turned to an external data source to understand the full range of crimes and security breaches at their facilities. Most often, this data is obtained directly from the source, such as local law enforcement agencies. Increasingly, companies are turning to third-party providers who compile the data into a useful format.

SCAN FOR CRIME PROBLEMS

12. Dust off your reports

A valuable source of data is in-house security reports. As the name implies, these are reports of criminal activity and other incidents (parking, loitering, and security breaches) which may be of concern to security professionals. This information should be reviewed by security professionals on a regular basis while looking for trends and patterns that might indicate existing threats or point to a vulnerability that can be solved with remedial measures. Security incident reporting typically include the following elements:

1. Incident reported
2. Date of incident
3. Time of incident
4. Precise location where the incident occurred on property.
5. Victim(s), if any
6. Witness(es), if any
7. Modus Operandi (MO), or Method of Operation used by perpetrator, if any
8. Follow up investigation(s)
9. Remedy

The validity of security report data is only as good as the policy which outlines the reporting and recording procedures, the quality of supervision over security personnel, and the verification process used to eliminate subjectivity. Regardless of the quality of their security reports, security professionals should be cautious not to exclude other sources of data and rely solely on in-house security reports.

13. Avoid Social Disorganization

Demographics as a driver for security measures have been used at times in the industry. The basis for this is eighty year old research on *social disorganization* (Boba, 2001). Social disorganization models, as used today, consider the demographics of *large* areas (census tracts) to determine the risk of crime at *specific sites*. Demographic characteristics include race, education, income, housing, and population characteristics. The primary source for demographics is the Population and Housing census which is collected every ten years (US Census Bureau, 2009).

There are three reasons for not using demographics for optimizing security at specific sites. First is the obvious – demographic data is not crime data. The census bureau collects demographic information, *not* crime information. "The Census Bureau releases some statistics on the criminal justice system in our data on government employment and finance, but none on crime, criminals, or victims" (US Census Bureau, 2009). Second, social disorganization models provide no site-specific data to indicate an actual crime rate at a specific property. For example, social disorganization models cannot tell us what occurred at 123 Main Street, Houston, Texas. The social disorganization model can tell us only what the demographics are for the census tract in which 123 Main Street is located. Census tracts are too large, each averaging about 4,000 inhabitants (US Census Bureau, 2009), to be useful for designing effective security programs. As discussed above, the greatest preventive benefits will result from focusing resources on high risk sites because crime is heavily concentrated on particular people, places and things (Eck J. E., 2007). Third, making security decisions for a particular site based on information for large areas such as census tracts may expose an organization to liability. In consideration of the *Daubert* factors discussed above, Courts may reject demographics, or rather the models that use them, in negligent security litigation. In a recent case, the social disorganization model was challenged under *Daubert*. The social disorganization model was used by the security expert retained by the defendant company. Opposing counsel argued before the Court that the defense's security expert:

1. could not offer any evidence that his methodology [the social disorganization model] had been subject to peer review or publication;

2. acknowledged that his methodology had not been tested;

3. stated that the methodology did not have a known error rate; and

4. could not identify any evidence suggesting that his methodology was generally accepted by a relevant professional community.

As the above example illustrates, a *Daubert* challenge would make defending a negligent security lawsuit difficult for any company that solely use a social disorganization model to drive their security program. Using an unpublished methodology that has not been subjected to peer-review and has a high error rate, the social disorganization model purports to predict the risk of murders, rapes, robberies, assaults and other crimes based on the demographics of the area population. But it can't tell us what has occurred, when it occurred, where it occurred, or how it occurred at a specific property. "While there is the potential for the police to link crime data, and the incidence of specific crime types, with information about the socio/economic status of the local population, there are problems inherent in such data." (Read, 1995).

Though the accuracy rate for the social disorganization model is not known as the model is not published or peer-reviewed, it is lower than crime data. One study indicates that calls for service over a year's period has a 90% accuracy rate, significantly higher than demographic data, in predicting crime in the long run (Eck, 1995).

14. Make friends with law enforcement

Law enforcement data is the most widely used source data for crime analysis because it presents an accurate crime history for a property and is from objective source. Since law enforcement agencies don't have a stake in a company or any associated liability exposure, their crime data is generally considered reliable and unbiased. Though some instances of crime statistics manipulation have occurred historically, rarely if ever, are the statistics for specific properties skewed. Most crime data manipulation occurs at a macro level with the objective of serving political or social goals. At the property level, there is little reason for law enforcement agencies to skew the statistics.

The data needed for crime analysis is site specific and has pertinent information regarding the nature of the crime, the date and time of the incident, offense report or case numbers, and disposition of the incident. The source data for crime analysis is comprised of either Uniform Crime Report (UCR) or Calls for Service (CFS) and Offense Reports. Each of these is described in detail below.

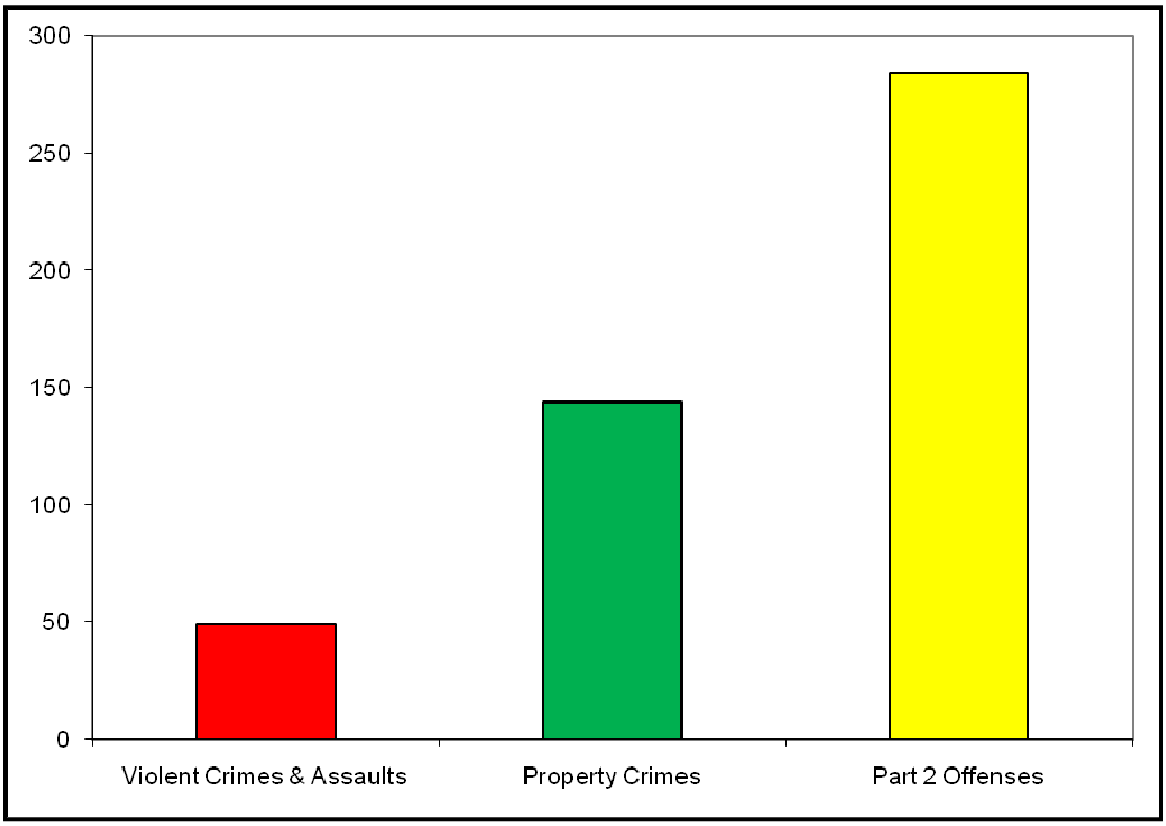
15. Meet the feds

The Federal Bureau of Investigation's Uniform Crime Report (UCR) system collects and maintains crime statistics from law enforcement agencies across the country. While the UCR data is not available on a site specific basis in most police jurisdictions, an increasing number of police departments are moving to advanced crime analysis systems which do allow for site specific UCR data. If UCR data is not available for the subject site, there are alternatives (see Calls for Service and Offense Reports below). The importance of the UCR is not its availability for specific sites, but rather that it provides the framework for consistent and uniform definitions of crimes (Federal Bureau of Investigation, 2004). Using the UCR definitions, a security practitioner can accurately compare crimes across different jurisdictions. The UCR framework defines twenty-four crimes as seen in the table below:

Category		UCR Code	UCR Name
Part I Offenses	Violent	1	Criminal Homicide
		2	Rape
		3	Robbery
		4	Aggravated Assault
	Property	5	Burglary
		6	Larceny – Theft (except motor vehicle theft)
		7	Motor Vehicle Theft
		8	Arson
Part 2 Offenses		9	Other Assaults
		10	Forgery and Counterfeiting
		11	Fraud
		12	Embezzlement
		13	Stolen Property-Buying, Receiving, Possessing
		14	Vandalism
		15	Weapons - Carrying, Possessing, etc
		16	Prostitution and Commercialized Vice
		17	Sex Offenses
		18	Drug Abuse Violations
		19	Gambling
		20	Offenses Against the Family and Children
		21	Driving under the Influence
		22	Liquor Laws
		23	Drunkenness
		24	Disorderly Conduct
		25	Vagrancy
		26	All Other Offenses
		27	Suspicion
		28	Curfew and Loitering Laws
		29	Runways

The first four crimes (murder, rape, robbery, and aggravated assault) are defined by the Federal Bureau of Investigation as violent crimes. Murders, rapes, aggravated assaults and assaults are considered to be *crimes against persons*. While, robbery involves a present victim, it is technically classified as a crime against property; however, it is a violent crime. The second group of four crimes (burglary, theft, auto theft, and arson) is grouped as property crimes.

Crimes 10 to 24 are referred to as Part 2 offenses. The following graph displays a typical breakdown of the crime groups:



Crime in the United States, accessible via the FBI's website, provides statistical breakdowns of these crimes for cities and counties. Unfortunately, city and county level data is not specific enough for crime analysis. In some rare jurisdictions, UCR data for the property level is available from the law enforcement agency. Where available and if provided with dates and times, site specific UCR data streamlines the crime analysis process.

In most cases, however, site specific UCR data level will not be available and an alternative approach must be taken. That alternative approach is to recreate the UCR for the specific site, which is easily accomplished through use of Calls for Service (CFS) and Offense Reports. CFS and Offense Reports provide sufficient information to recode each incident using UCR codes and definitions. The primary benefit of this is that sites may be compared across law enforcement and legal jurisdictions where crime definitions may vary.

16. Review the call logs

CFS are a listing of all reports called into the police from the property and normally include the reported incident, the date and time the call was made, and an incident number. In some cases, calls for service also tell us whether there was an offense report written, the disposition of the case, and possibly the UCR classification. In essence, CFS disclose the initial details of crimes reported to the police from a particular location and include every report of crime, suspected crime, and other activity as reported by a victim, witness, or other person to a local law enforcement agency.

Calls for Service are those crimes or other activity reported by a victim, witness, or other person to a local law enforcement agency via 911 emergency system and other channels. These reports may consist of actual crimes, from murder to theft, or suspicious activity, and other incidents such as missing children, motor vehicle accidents, and parking complaints. Whatever the concern, if it is reported to law enforcement, the CFS records will likely include this incident. Typically, the synopsis of the given incidents is included on the record along with the location, date, and time the event was reported.

Some newer CFS systems encode data using the Federal Bureau of Investigation's Uniform Crime Report codification system, thus crimes can be easily differentiated from false reports and easily compared to city, state, and national crime levels. Older systems, though, must be converted to UCR through verification with offense reports.

CFS data reflects from the location where a complaint was made, which may or may not be the site of the incident. However, the location and precise nature of the calls can be verified and reliability enhanced when CFS are used in conjunction with offense reports.

17. Validate the calls

More of an expansion of Calls for Service than an independent data source, an offense reports is the written narrative of a call for service that resulted in an actual crime. Offense reports are the written narrative of a crime investigation and are used to verify CFS. This verification process is necessary as CFS data reflect the location from where a complaint was made, not necessarily the incident location. Offense reports also confirm the type of crime committed as well as the date and time of the offense. In many jurisdictions, only select portions of the offense report are available, however, there is usually enough information contained in the public information section to accurately build a database of crime incidents.

18. Apply your expertise

CFS, Offense Reports, and UCR data have been discussed as the best options for analyzing crime trends at a facility. While those sources are important for understanding *what has happened*, they do not consider *what could happen*. While many security professionals subscribe to the axiom, t*he best predictor of the future is the past*, threats that have not exposed themselves yet should also be considered. To address what could happen, and though not the focus of this report, inherent and conceptual threats should be assessed.

Inherent threats are defined as "threats that exist by virtue of the inherent nature or characteristics of the facility or nature of the operation" (International Association of Professional Security Consultants, 2008). For example, certain types of facilities or assets may be a crime magnet or prone to loss, damage or destruction (e.g., assaults among patrons in nightclubs, infant abductions from hospital nurseries, etc.). Inherent threats consider the attractiveness or value of assets. Certain assets and businesses have a higher inherent threat level because of their inherent attractiveness to the criminal element. One example is jewelry stores. Despite no previous crimes at a particular jewelry store, the threat level for robberies and burglaries is still high. This is not to say that jewelry stores are inherently vulnerable, only that the inherent threat level is higher. Another example of a business with an intrinsically elevated threat level is construction sites which typically have a higher rate of accidents resulting in injury to workers when compared to other sites. Assets that are small, portable, and saleable may also elevate the inherent threat level. Examples of this include computer parts such as RAM and processors or in the healthcare environment, durable medical equipment may have a higher inherent threat level. Again, the threat exposure may exist, but the vulnerability may not.

Conceptual threats, or potential threats, are defined as "threats which exist by virtue of vulnerabilities around the asset or weaknesses in the security program which produce opportunities for crime to occur" (International Association of Professional Security Consultants, 2008). Conceptual threats are primarily identified via a vulnerability assessment. An example of a conceptual threat may be theft from a loading dock. During an inspection, the security manager found an unsecured pedestrian door to the loading dock that may be accessed by criminals to steal items from the loading dock.

Conceptual threats may also be identified through information sharing among industry peers. Banks, for many years, have shared information amongst themselves on bank robbery suspects. In more recent years, retailers have been more willing to share information on organized retail theft. This sharing information may be done informally local directors meeting for lunch or more formal via industry security associations.

ANALYZE IN DEPTH

"Research has shown that crime is seldom randomly distributed across an area, rather there are marked geographical and temporal skews in the patterning of offence locations, often varying according to the type of crime" (Read, 1995).

The crime analysis methodology outlined below is based on a logical foundation and provides useful information for a security professional. By no means is the methodology limited to what is described, as to a large extent, security professionals may find that the information requires customization to meet company needs.

Though crime analysis can be conducted using paper and pen, a software application, such as a spreadsheet, is recommended for quicker data entry, sorting, and analysis. Software applications also allow users to easily create graphs, charts, and maps. A typical spreadsheet will start with keying in basic elements (Vellani, 2001) from the CFS and offense reports, including:

- Site (address and/or site number)
- Reported Crime - This information is located on the CFS sheets and may also be listed in the offense report
- UCR Code - Since most police departments do not include this code, this may be inserted later
- UCR Description/Actual Crime Committed - The first page of the offense report will normally have the final crime classification
- Date - This is the date on which the crime occurred, not the date reported
- Time - This is the time at which the crime occurred, not the time reported
- Day of Week - This may be inserted manually if not listed on the offense report
- Offense Report (or Incident) Number - Listed on the offense report
- Crime Location - This is a description for advanced analysis and may not be known or gleaned from the offense reports. As mentioned earlier, in reviewing a crime scene location, it is often important to determine whether the crime is internally or externally generated.

Once all the information from the data sources are entered into a spreadsheet, the crimes should be coded uniformly to ease comparison across law enforcement jurisdictions. The UCR coding system is ideal.

Using a spreadsheet or database, security professionals can sort information by site, by type of crime, by date, time, or day of week. The database will also allow the security professional to begin performing basic calculations such as totals for specific types of crime at each site and the average crimes per site. One may also be able to discern any patterns or trends in crime types or temporally (date, time, day).

Crime rate analysis, time series analysis, modus operandi analysis, and pre-test/post-tests are among the more useful types of analysis. More advanced analysis types (crime specific, hot spot, and thresholds) are discussed in the Future Responses section later in this report. Each of these types examines different aspects of crime's impact at a facility and indirectly identifies appropriate countermeasures to the known risks. Each type seeks to find a trend. "A crime trend is defined as a significant change in the nature of selected crime types within a defined geographical area and time period. The analysis is concerned with changes in the fundamental crime pattern, and involves comparisons of aggregated crime data sets over time" (Read, 1995).

19. Compare apples to apples

Crime rates provide context to absolute crime levels. Crime rates are one of the best methods for comparing crime at various facilities. Crime rates should be used whenever possible as they offer the most accurate reflection of crime at a site by taking not only the crime level into account, but also the population or traffic level of the facility (Gottlieb, 1998). By utilizing the population or traffic levels, a security professional is able to make apples-to-apples comparisons of facilities under his or her control, to similar businesses in the area, and to larger geographic areas such as the city in which the facility is situated.

The traffic level, or population of the facility, is used to calculate violent crime rates. Determining the population of a property depends on the type of facility. Population reflects the number of persons at a property. Generally, there are two schools of thought. The easier of the two to identify the population is one where the population is generally stable throughout the day. An example may be an industrial facility or data center where people arrive in the morning and remain on site until the late afternoon. As another example, an apartment complex may use 2 residents per one-bedroom apartment unit and 3 residents per two-bedroom apartment unit. Thus, for a 100 unit apartment building which has 50 two bedroom

units and 50 one bedroom units, the population of the apartment building would be 250 people:

2 people x 50 one bedroom units = 100 people
+
3 people x 50 two bedroom units = 150 people
=
250 people

The second school applies to the facility with a more transient population where people arrive and depart many times during the day. Examples of this include retail stores, banks, and transportation hubs. One large fast food restaurant chain uses a standard number of customers per transaction based on historical records for the entire company. For every transaction, there are on average 2.1 people. Thus, if the restaurant has a daily transaction count of 4,000 transactions, they will have had 8,400 persons through the restaurant on that day.

2.1 people x 4,000 transactions = 8,400 people

In an effort to take geographic variables into account, some companies use a different multiplier for each region or district. Though this is more accurate, the multiplier may be difficult to discern. Security professionals should use whatever multiple is reasonable.

Once the population is known, the crime rate is calculated by dividing the number of crimes by the traffic level and then multiplying by 1000, the number commonly used to compare crime rates across the various levels of geographic analysis.

Property crime rates, on the other hand, use the number of property targets as the denominator. Most calculations of crime rates are not estimates of crime risk because inappropriate measures of the crime opportunities (targets) are used for the denominator in the calculations. For example, burglary rates are calculated by dividing the number of burglary events by the population of the area being studied. The appropriate denominator is the number of buildings in the area. An example of an auto theft rate is:

Formula: Auto Theft Rate = (Total Auto Theft/Population) x 1000

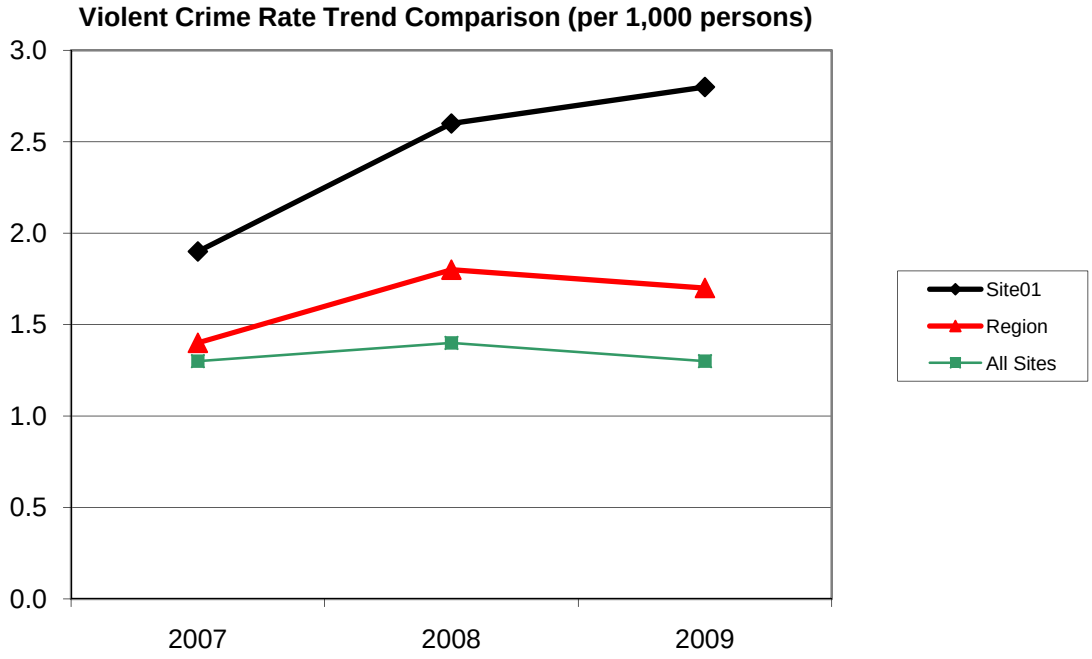
Number of Auto Thefts = 17
Number of Autos (targets) = 3500

Auto Theft Rate = (17/3500) x 1000
Auto Theft Rate = (0.00486) x 1000
Auto Theft Rate = 4.86

Crime rates should be calculated using the number of targets as the denominator (Gottlieb, 1998). In other words, for crimes against persons or violent crimes, the denominator should be the number of persons. For crimes against properties, the denominator should be the number of items under consideration.

Comparisons may also be made to other geographic areas for which crime statistics are available including census tracts, police beats, metropolitan statistical areas, states, and the nation as a whole). It is important to note that the larger the geographic area, the less relevant the comparison. Crime analysis emphasizes the smallest geographic area possible, the property level.

Using the crime rate formula allows one to accurately compare threat levels at different sites, or compared to a geographic area, or to all similar sites. The formula may be applied to each year (or other time period) to trend crime over time to discern whether crime is increasing, decreasing or is stable (see graph below).



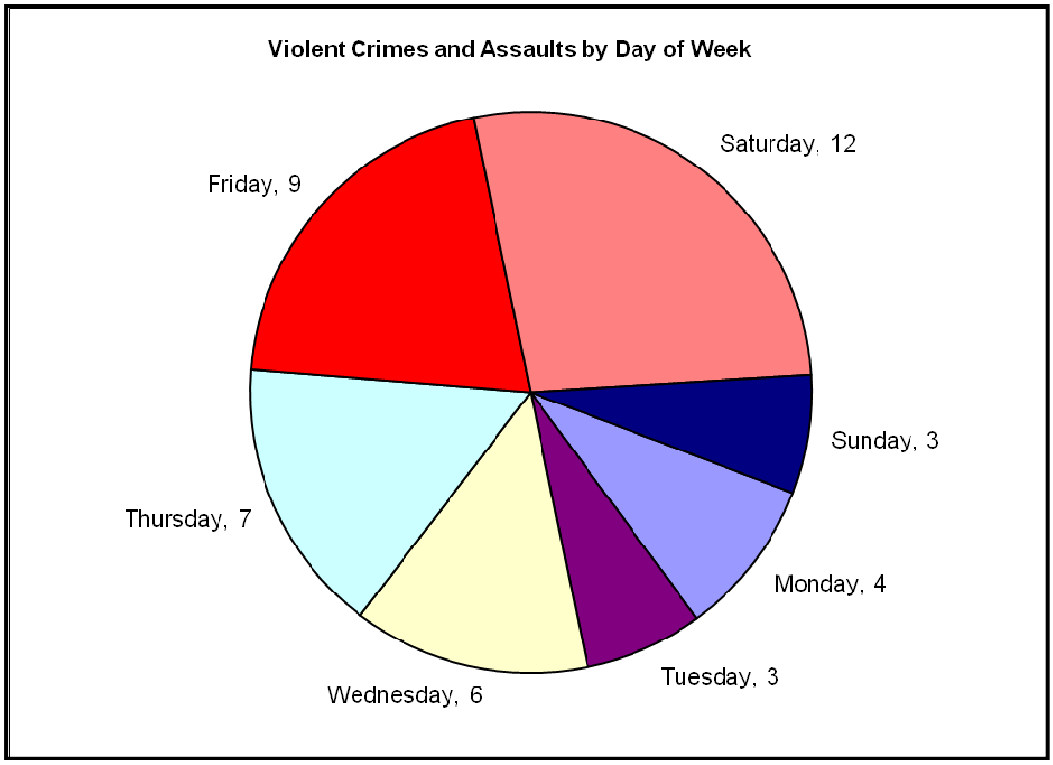
20. Clock your crime

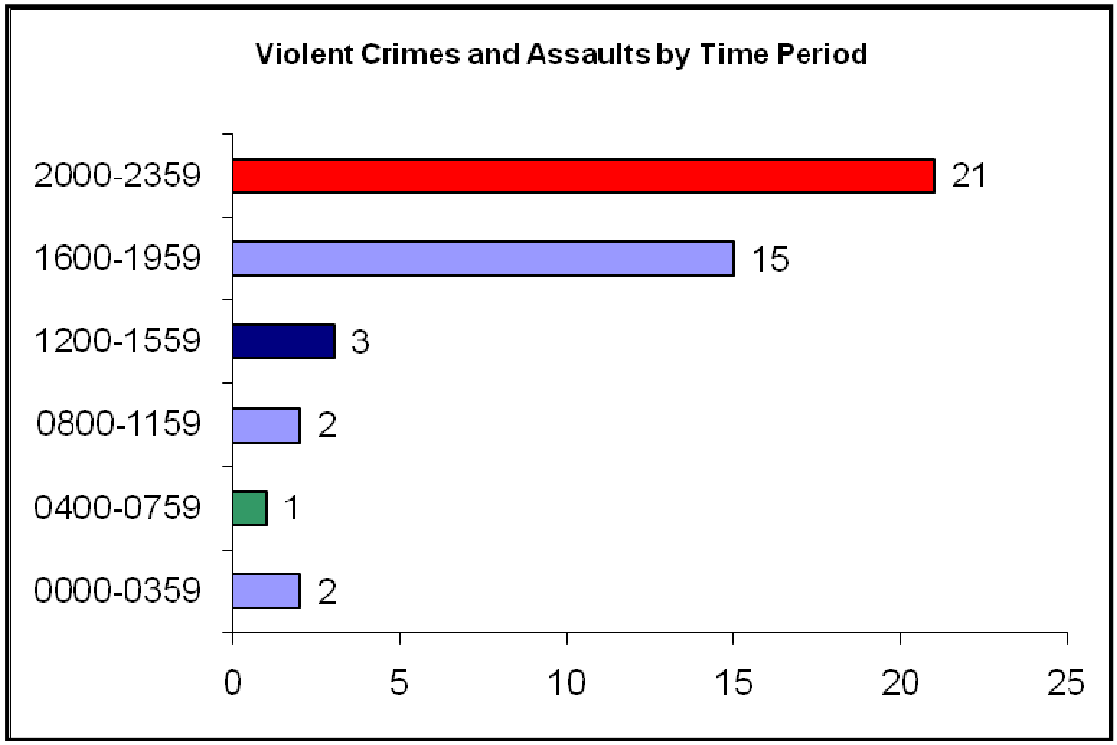
Once high threat facilities have been identified using crime rates or absolute crime levels, trends *over time* may be identified for individual facilities or for aggregated facilities (e.g. region, all facilities, state, etc.). Time series analysis, or temporal analysis, is used in crime analysis to trend crime over time and provides a breakdown of crime at specific time intervals (e.g. year, day of week, quarter, etc.). Understanding *when* crimes occur is important to optimize the security program for individual facilities. "The basic principle is to obtain a good idea of a problem's natural trends, cycles, and variation before the response is implemented." (Clarke, 2005).

Time series analysis may identify particular crimes that occur during certain periods. Crime trends by day of week, time of day, season, or year can drive scheduling decisions. As threats increase, security may be increased. As threats decrease, coverage may be reduced. Deploying security measures during high crimes times and reducing security during low threat times can generate savings and demonstrate a return on investment. Though other security practices can be adjusted and modified based on temporal analysis, it's most common use is in the efficient scheduling of security personnel. Time series analysis can significantly cut down the cost of a security force.

Time series analysis can overcome assumptions or gut instincts about crime. For example, a retail store manager may approach his company's security manager and request additional security on Friday and Saturday nights to protect against crime. The analysis may indicate that crime increases on Thursdays and Fridays, rather than Fridays and Saturdays. Similarly, a time series analysis may indicate that crime is evenly distributed over days of the week at a specific property, but the vast majority of the crimes occur between the hours of 4pm and 4am. This knowledge helps decision makers efficiently deploy security resources, security officers in particular. "Many practical questions are answered through trend calculations and these assist in the decision making process" (Gottlieb, 1998).

There are many ways of analyzing temporal trends, but the most common are day of week, time blocks, monthly and quarterly, and annually. In the Day of Week graph below, a clear trend is evident on Thursdays, Fridays, and Saturdays. One those days, we may deploy security or additional security personnel. On the Time Period graph, a crime trend is evident between the hours of 4pm and midnight.





21. Assess the MO

Modus Operandi is a term commonly heard in television crime dramas and refers to the method of operation, or MO, used by a criminal perpetrator. Crime profilers often use the term *signature* when referring to a criminal's modus operandi. MO analysis answers the *who* question. Who committed the crime? Depending on the availability of details in internal security reports, offense reports, or interviews with victims, witnesses, and offenders, MO analysis determines an offender's criminal tactics that separate their crimes from other criminals.

From modus operandi analysis, certain crime features become known. Some crimes such as purse snatchings on days when people are paid might make sense when one considers what has been learned about rational choice theory and routine activity theory[1], or that home burglaries tend to occur when the home is unattended or that shoplifting tends to occur more frequently when a business is sparsely staffed. If such a fact in a given area is known and known enough by criminals, then the seed of criminal activity can be planted and come to fruition when such times arrive. Such occurrences happen for a reason.

22. Mimic the weight loss commercials

A pre-test / post-test is a good method for measuring the effectiveness of a security program. Not unlike the before and after photographs shown in weight loss commercials, a pre-test / post-test measures crime before the implementation of new security measures and then re-measures crime sometime after implementation. While the math involved with this test is scientific, the results are not wholly scientific, but are useful nonetheless.

An example of valid results may be found in US national security. The implementation of many security measures (policy, training, physical, electronic, and personnel) in American airports has prevented a recurrence of 9/11 style attacks. While valid, the results are not scientific as all the factors relating to such a crime are not considered.

On a more practical level, common crimes such as theft or burglary, lend themselves to better pre-test / post-test analysis. A retail store which implements a comprehensive organized retail crime prevention program may be able to measure losses for two years prior to

[1] For an excellent primer on Rational Choice and Routine Activity Theories, please see: Clarke, Ronald V. and Felson, Marcus (1993). Routine Activity and Rational Choice. Advances in Criminological Theory, Volume 5. New Brunswick, NJ: Transactions Publishers.

implementation of the program, and then measure loss two years after implementation. The results may show a dramatic decrease in loss that, at least in part, may be attributed to the program.

In early 2007, the author assessed an apartment complex which included an analysis of both historical and conceptual threats, a vulnerability assessment (security survey), and an inventory of current security measures. The historical threats were analyzed by reviewing crime information from the police department for the years 2004 to 2006. Based on the number of violent crimes, assaults, and property crimes, there was a significant threat of more crime on the property. A report was generated which included twelve recommendations for enhancing and optimizing the security program. Two and one-half years after the report was delivered, the client called on the author to conduct a follow up assessment. The follow up assessment verified that most of the recommendations had been implemented. The most significant change was the security personnel contractor. Security officers displayed greatly improved professionalism. Their morale was much higher when compared to the prior assessment and clearly, they were interested in doing their job and doing it well.

Quantitatively, the updated threat assessment reflected a 43% decrease in property crimes and a 50% decrease in violent crimes and assaults during the first year following the initial assessment and a further decline in violent and property crimes in year 2. Beyond the crime data, there was also evidence of qualitative improvements. Residents of the complex appeared to have less fear of crime as the common areas were being used as gathering points for adults, residents were seen washing cars in the parking lots, and most telling was the number of children playing in the complex's playgrounds (parents typically don't let young children play outdoors when fear of crime is high). During the initial assessment, there was little to no use of the common areas by legitimate users. The apartment manager confirmed that resident complaints were much lower and that her staff was no longer fearful of walking the property.

The follow up report contains recommendations for further enhancing the security program, but also an opportunity to reduce security expenditures by approximately 17% based on the reduced crime level. The savings could be generated by decreasing security personnel coverage during low threat times. While this example is anecdotal, it demonstrates that security can be optimized to realize a return on investment, but more importantly it demonstrates how to conduct a pre-test / post-test.

23. Be specific

It is still common today to analyze violent crimes as one group and property crimes as another. Noted criminologists Ronald V. Clarke and John E. Eck admonish crime analysts to “be very crime specific” (Clarke, 2005). Crime-specific analysis addresses the *What* and *How* questions to aid countermeasure selection. Security professionals can use crime analysis to select specific measures as indicated by the data.

Crime-specific analysis helps drive those decisions. If the specific crime types are known, better solutions may be formulated. The following examples illustrate the point:

1. Shoplifting escalation robberies reduced through employee training
2. Car-jacking robberies reduced through lighting and parking lot design
3. Purse snatching robberies reduced through customer awareness
4. Apartment “door kick” home invasion robberies reduced through perimeter access control

In all four examples, the primary crime is robbery. However, the specific type of robbery drives the decision to deploy one countermeasure over another. Clarke & Eck state that “the differences between crimes explain why the solutions to each cannot be the same” (Clarke, 2005).

Though the FBI’s UCR coding system breaks crimes down into their specific legal elements, it is often beneficial to break crimes down into sub-levels for security purposes. "Because so much effort has been concentrated on crude groupings of crime types, such as burglary, robbery or auto theft, it has been virtually impossible to find truly common facts about the conditions which lead to each of these groups of crimes" (Clarke, 2005). Crime-specific analysis gives security professionals more information to develop better solutions. Using this type of analysis, one can analyze individual crime types (robbery, theft, burglary, etc.) and further refine the analysis with sub-types (shoplifting escalation, car-jacking, purse snatching, home invasion, etc.). Crime-specific analysis can tell us whether the robbery victim was a business or an individual. This specificity aids in understanding the nature of the problem, to what degree it exists, and indirectly what security measures can be used to reduce the opportunity for those problems.

Another benefit of this type of analysis is that a breakdown by crime will help to indicate whether the asset targeted was a person or property, whether the crime was violent or not, the resulting loss or damage to that particular target, and the implications of that loss or damage. As already mentioned, this data should be coded in compliance to the FBI's Uniform Crime Report system for ease of comparison among properties and to create uniformity among the data sets. However, further information may be included beyond the UCR code and description including victim type, asset targeted, and location of crime.

In protecting people, security measures are typically not deployed to prevent or deter domestic or interpersonal violent crimes. Interpersonal crimes, or expressive crimes, usually result from impulsive reactions to events carried out in the heat of the moment (Wortley, 2008). Interpersonal and domestic crimes are more often prevented via social measures, not security measures. A battered women's shelter, for example, is designed to keep batterers away from the victims of spousal abuse. Anti-bullying policies in schools are used to prevent students from bullying other students. Both are social measures, not security measures.

In contrast to social measures, security measures are deployed to protect legitimate users of a property from unknown criminals. Despite the fact that security measures are primarily deployed to protect against stranger-initiated crimes, it should be noted that security measures can sometimes intervene in interpersonal events once initiated.

The distinction between interpersonal crimes and stranger-initiated crimes is:

- Interpersonal is defined as being, relating to, or involving relations between persons (Merriam Webster, 2009). Interpersonal crimes are those that occur between known parties and include domestic crimes as well as other crimes where the victim and perpetrator are known to each other.

- Stranger-initiated crimes are those that occur between unknown parties. They are more often instrumental crimes, planned attacks with a clear purpose (Wortley, 2008).

When assessing the risk of violent crimes, a reasonable attempt should be made to separate interpersonal crimes from stranger-initiated crimes. The primary method for separating the two is to review the offense report generated by law enforcement. The narrative of the report will often indicate whether or not the victim and suspect are known to each other. In some reports, domestic crimes are clearly marked, while in others, the narrative may identify the relationship between parties. Other relationships, such as friends, roommates, classmates, boyfriend/girlfriend, typically do not have a "check box" but can sometimes be discerned via the narrative.

24. Push your pins

Hot spot analysis identifies *where* crimes occur on the property. Understanding where crimes occur, particularly on large facilities, helps deploy security in the right places. Examples of "spaces" include parking lots, interior public spaces, private secured spaces, bridges connecting buildings, etc. Hot spot analysis is concerned with *wheredunit* rather than *whodunit*.

Hot spot analysis identifies small places in which the occurrence of crime is so frequent that it is highly predictable. Hot spots are identified using clustering, that is repeat events or crimes at the same place. Hot spots have higher risk and a higher number of crimes when compared to other similarly sized areas (Wortley, 2008). "This phenomenon is commonly called the 80-20 rule; where in theory 20 percent of some things are responsible for 80 percent of the outcomes" (Clarke, 2005).

Since the purpose of this Report is to establish a framework for security optimization on a site specific basis, much of the research on spatial analysis does not apply as that research has a primary focus on community level interventions, not "place-specific" interventions. However, there is some literature on spatial concepts that are relevant to a site specific analysis. Logic also helps. Floor plans will be more useful than maps for site specific analysis.

In a small facility (e.g. convenience store, bank branch, etc.), all that may be necessary is that security practitioners know whether crimes are occurring inside the building or out in the parking lot. In an apartment complex, where property management is responsible primarily for the common areas, not inside the apartment units, understanding the nature of crime in the common areas is more helpful in optimizing the security program.

On larger facilities, such as office towers, hospitals, and university campuses, a more sophisticated analysis may be necessary. Eck and Clarke (2005) identify three kinds of hot spot places. On a large property, one or more of these may exist. First, crime generators are places with high levels of legitimate traffic. On a university campus, the athletic facilities (e.g. stadium, fields, etc.) are examples of crime generators. Second, crime attractors are places that have a high number of targets. On a hospital campus, parking garages provide ample opportunity for auto thefts and vehicle burglaries. Third, crime enablers are places with a low level of "place" management. Campus parks may not be supervised (Clarke, 2005, Wortley, 2008). Paul and Patricia Brantingham identify a fourth concept, the crime neutral areas. Crime neutral areas are not hot spots and are spaces that don't attract targets, offenders and behavioral controls are sufficient (Brantingham, 1995, Wortley, 2008).

Rengert, Mattson, and Henderson used High-definition Geographic Information Systems (GIS) to provide a more meaningful analysis for crimes on university campuses. To test the effectiveness of security measures, Rengert et al used high definition GIS to measure crime around "points," that is unique features that act either as an attraction to crime (e.g. automated teller machine) or a repellant (e.g. police kiosk). Their analysis, using high definition GIS, found that police kiosks significantly reduced crime around the kiosk significantly (Rengert, 2001). Clearly, high definition GIS has uses for measuring effectiveness of security measures on large campuses such as university campuses, hospitals and medical centers, as well as closed environments such as data centers and chemical facilities.[2]

25. Ring the bell

Not all crimes can or will be prevented. As such, organizations, as part of their overall security plan, should identify acceptable threat levels at a given facility. The plan should include "criteria for establishing 'threshold' levels for identified crimes and criminal activity" (Woods, 1999). "The reason we establish crime thresholds is to provide an objective basis for determining when crime is getting out of hand" (Gottlieb, 1998). Security professionals "need to know the upper and lower limits (known as thresholds) of each crime in order to determine if they are either within, above, or below their expected levels" (Gottlieb, 1998).

A threshold analysis provides the basis by mathematically calculating the "normal" levels of crime for a facility or group of facilities. This analysis is most useful when comparing like facilities in similar environments. A high threshold is the upper limit of "normal" crime for selected sites, while a low threshold is the lower level for selected sites. Thresholds may be calculated using the standard deviation of selected sites with the following formulas:

High Threshold = Mean Crime of Selected Sites + 1 Standard Deviation

Low Threshold = Mean Crime of Selected Sites - 1 Standard Deviation

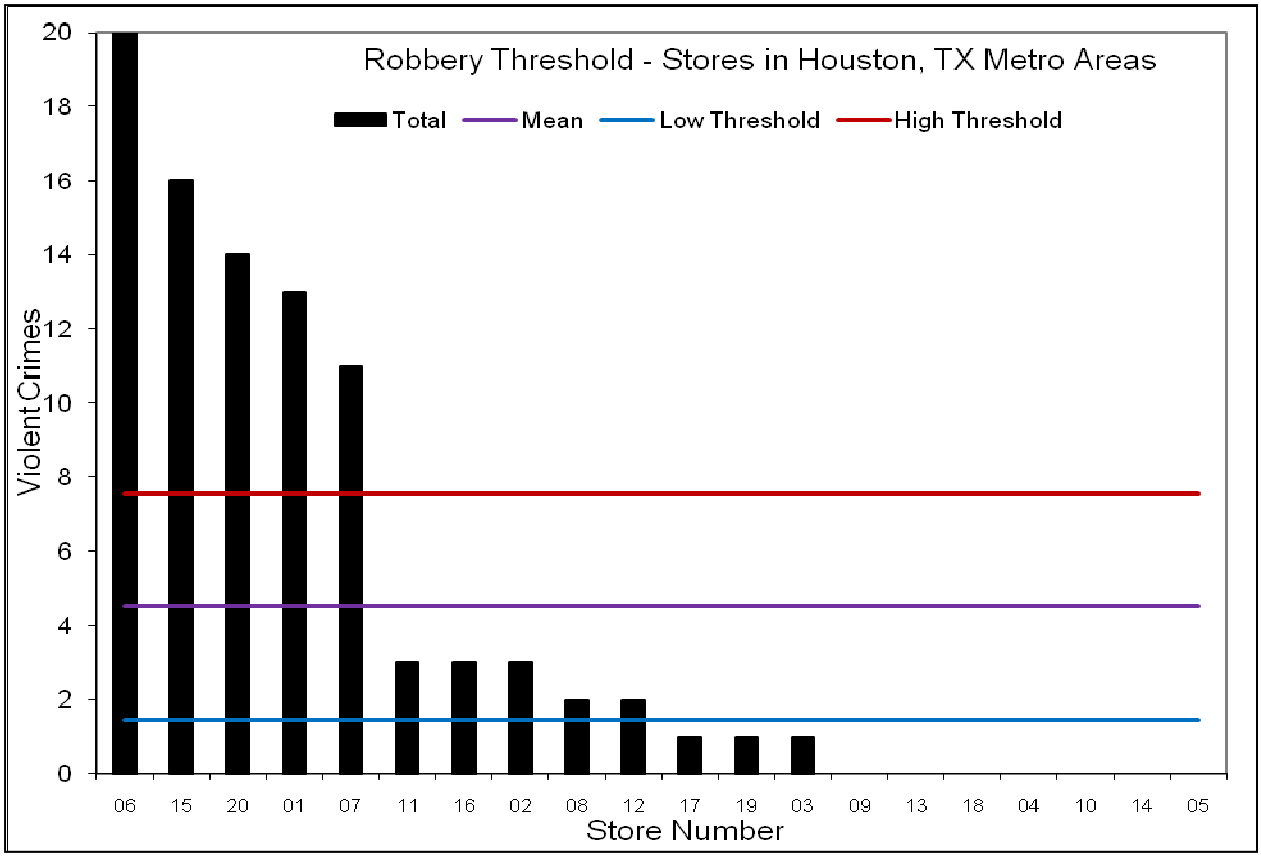
It should be noted that standard deviation is an arbitrary indicator, but when applied uniformly across similar facilities, it provides a good baseline for comparison. Other indicators may be used as dictated by the needs of the analysis.

[2] For more information on high density GIS, see Campus Security: Situational Crime Prevention in High Density Environments by George Rengert, Mart T. Mattson, and Kristin D. Henderson.

The following example is for a retail chain with twenty stores. All twenty stores are located within the metropolitan area of a large urban city. During a three year period, the stores experience a range of robberies as seen in the table below:

Store	Robberies
06	20
15	16
20	14
01	13
07	11
11	3
16	3
02	3
08	2
12	2
17	1
19	1
03	1
09	0
13	0
18	0
04	0
10	0
14	0
05	0

Based on the crime data for each store, the average (mean) number of robberies is 4.50 per store. The data can be used to calculate a standard deviation of 3.06. Using the formula above, we can calculate a high threshold of 7.56 and a low threshold of 1.44. This information is best illustrated graphically as in the example below.



In this example, the black columns represent the total violent crimes per store during the three years. The purple line represents the average number of robberies. The red line represents the high threshold. The blue line represents the low threshold. Relative to its peers, any store that rises above the red line is mathematically high crime, while any store that drops below the blue line is low crime. Stores which fall between the blue and red lines are considered average (Gottlieb, 1998). The heavy concentration of crime on the left side of the graph, referred to as Power Law or more commonly as the 80/20 rule, shows that applying countermeasures to the "high crime" stores will yield the most benefit. This distribution is referred to as a "J" curve (Eck J. E., 2007). In the example above, 85% of the robberies occurred at 25% of the sites. Eck, et al found similar distributions (J curves) across various data sets including 20.3% of stores experiencing 84.9% of shopliftings and 19% of motels contributing to 51.1% of calls for police service (Eck J. E., 2007).

RESEARCH NEEDS

Currently, there are a number of books available to public law enforcement on crime analysis, but there are a limited amount of texts available to private sector practitioners. In this era of community policing, there is an emphasis on cooperation among the security and law enforcement and many activities can be conducted by both to increase crime reduction productivity. Private security professionals and facility managers are just two segments of the private sector that greatly benefit from crime analysis. More research that teaches the private sector how to collect and analyze law enforcement data specific to their facilities would be a step in the right direction. In the end, improved cooperation and sharing of resources and tools will result in both the private sector and the public sector benefitting with lower crime.

The literature on crime analysis is also lacking in basic theoretical foundations that explain how crime analysis helps us prevent crime. Though many practitioners have excelled far beyond the fact that crime analysis is a proven tool, there is always a need for texts which explain why crime analysis works and the best methods to implement crime analysis results. For the beginning crime analyst, new texts which provide the latest methods of crime analysis coupled with the theoretical foundations will help them become very productive.

The future of crime analysis literature should be geared toward a complete manual of "best practices" in crime analysis methodologies. There have been concrete steps in this direction (see ASIS-International's General Security Risk Assessment Guideline or the International Association of Professional Security Consultant's Forensic Methodology), no single guideline has been published by an industry association that solely describes the crime analysis process for the private sector.

While Geographic Information Systems (GIS) systems have greatly improved crime mapping functionality in the public sector, few of these systems are designed for the private sector. The reason for this is that mapping generally is of little use to private sector professionals who are not responsible for an entire geographic area, but rather only individual facilities within the larger area.

Two major steps in the right direction for the security industry would be educate security professionals on the real limitations of demographics and social disorganization models as well as methods to incorporate other metrics into a crime analysis program, such as shrink / loss data as well as liability costs.

PRACTICAL APPLICATION OF CRIME ANALYSIS

The use and application of crime analysis to individual organizations will vary based on the organization's culture, business nature, and sophistication of the asset protection program. Most companies will derive benefits from crime analysis, either as a standalone tool or as part of a broader risk model, to drive their security programs and ensure that it operates at an optimal level.

One of the first decisions that should be made is they types of crimes that will drive the security program. Unlike property crimes, violent crimes physically impact people and sometimes result in serious bodily injury. From a liability perspective, violent crimes result in litigation more frequently than property crimes. Assaults, while not considered violent per the FBI definition, should also be included as they also impact people. Property crimes (burglary, theft, auto theft, and arson) may also be considered depending on the nature of the organization undertaking crime analysis. Some businesses make significant security decisions based on property loss, while others don't. Like other crime groups, the need to analyze Part 2 offenses (see Uniform Crime Report section) is highly dependent on the nature of the business conducted at the specific property. Forgery, a Part 2 offense, may be important for banks and retailers, but less so for hotels. Likewise, prostitution is likely of more concern at a hotel than it is at a convenience store. The crimes analyzed depend on the needs of the organization. Alternatively, an organization may choose to analyze all crimes.

Another decision that should be made when developing a crime analysis program is how often that data is analyzed. Since many security decisions, like most other business decisions, are based on budget years, crime analysis is most frequently conducted on an annual basis. Organizations that aggressively manage their security resources, that is make adjustments often, may benefit from more frequent intervals.

Like any project, allocating sufficient resources and skill is needed for a successful outcome. Since crime data from law enforcement agencies is a primary data set for crime analysis, time is the most critical resource. Depending on the jurisdiction, some agencies are able to turn requested data around in a day while others may take several weeks. If both calls for service and offense reports are needed, the process may take two or more months to complete. The number of sites to be analyzed is also a factor. Logic would dictate that the more sites, the more time that will be needed, especially if those sites are in different law enforcement jurisdictions. A company with fifty sites in twenty different jurisdictions will likely take more time than a company with fifty sites in two jurisdictions. The crime analysis methods outlined in this paper are easily conducted using standard office software applications. Rarely are advanced statistical

applications or mapping applications needed.

Another consideration for organization's implementing such a program is the weight of crime analysis should have as a security decision driver. Sophisticated security programs normally have a number of components that are also considered beyond threat data. Other considerations may be individual site budgets, unique site vulnerabilities or high value assets. More commonly, security practitioners have a multitude of elements that also drive the security program. These may include internal security reporting, conceptual threats, among many others. The weight of crime analysis within the organization's broader risk model is invariably tied to each organization's unique culture.

REFERENCES

ASIS-International Guidelines Commission. (2003). *The General Security Risk Assessment Guideline.* Alexandria: ASIS-International.

Bates, N. D. (2006). Premises Security Liability. In K. H. Vellani, *Strategic Security Management* (pp. 269-270). Boston: Butterworth-Heinemann.

Boba, R. (2001). *Introductory Guide to Crime Analysis and Mapping.* Washington, DC: U.S. Department of Justice.

Brantingham, P. a. (1995). Criminality of Place: Crime Generators and Crime Attractors. *European Journal on Criminal Policy and Research* , 1-26.

Brantingham, P. L. (1993). Environment, Routine, and Situation: Toward a Pattern Theory of Crime. In R. V. Felson, *Routine Activity and Rational Choice: Advances in Criminological Theory, Volume 5* (pp. 259-294). New Brunswick: Transaction Publishers.

Cavanagh, T. (2008). *Security Metrics as a Management Tool.* New York: The Conference Board.

Clarke, R. V. (2005). *Crime Analysis for Problem Solvers.* Washington, DC: U.S. Department of Justice.

Eck, J. E. (1995). *Crime and Place.* Monsey: Criminal Justice Press.

Eck, J. E. (2007). Risky Facilities: Crime Concentration in Homogeneous Sets of Establishments and Faclities. In K. J. Graham Farrell, *Imagination for Crime Prevention* (pp. 225-264). Monsey: Criminal Justice Press.

Ekblom, P. (1988). *Getting the Best out of Crime Analysis.* London: Home Office.

Federal Bureau of Investigation. (2004). *UCR Handbook.* Washington, DC: U.S. Department of Justice.

Felson, M. (2002). *Crime and Everyday Life.* Thousand Oaks: Sage Publications, Inc.

Goldstein, H. (2009). *What is POP*. Retrieved 11 12, 2009, from Center for Problem Oriented Policing: http://www.popcenter.org/about/?p=whatiscpop

Gottlieb, S. S. (1998). *Crime Analysis: From First Report to Final Arrest.* Montclair: Alpha Publishing.

Illuminating Engineering Society of North America. (2003). *Guideline for Security Lighting for People, Property, and Public Spaces (IESNA G-1-03).* New York: Illuminating Engineering Society of North America.

International Association of Professional Security Consultants. (2008). *Forensic Methodology (Best Practice #2).* Des Moines: International Association of Professional Security Consultants.

Jopeck, E. J. (2000, August). Five steps to risk reduction: Learn to identify and reduce risk by following these five steps. *Security Management* , pp. 97-101.

Kitteringham, G. W. (2001). *A study of two types of vertical crime pattern analysis in the commercial multi-tenanted high-rise structure.* Leicester: University of Leicester.

Martin Gill, T. B.-H. (2007). *Demonstrating the Value of Security.* Leicester: Perpetuity Research & Consultancy International LTD.

Merriam Webster. (2009). Retrieved August 17, 2009, from Merriam Webster Online Dictionary: http://www.merriam-webster.com/

Miethe, T. D. (1998). *Crime Profiles: The Anatomy of Dangerous Persons, Places, and Situations.* Los Angeles: Roxbury Publishing Company.

O'Shea, T. &. (2002). *Crime analysis in America: Findings and Recommendations.* Washington: U.S. Department of Justice.

Pastor, J. F. (2007). *Security Law and Methods.* Oxford: Butterworth-Heinemann.

Prentice Hall. (2009). *Glossary*. Retrieved August 18, 2009, from Criminology Today, 4E: http://www.prenhall.com/cjcentral/crimtoday4e/glossary/e.html

Read, T. &. (1995). *Local Crime Analysis.* London: Home Office Police Research Group.

Rengert, G. M. (2001). *Campus Security: Situational Crime Prevention in High-Density Environments.* Monsey: Criminal Justice Press.

School of Criminal Justice at Rutgers University. (2009). *Underlying Theories*. Retrieved August 18, 2009, from Crime Prevention Service for Business: http://crimeprevention.rutgers.edu/topics/SCP%20theory/theory2.htm

The National Fire Protection Association. (2005). *Guide for Premises Security (NFPA 730).* Quincy: The National Fire Protection Association.

Tilley, N. (2002). *Analysis for Crime Prevention.* Monsey: Criminal Justice Press.
US Census Bureau. (2009, September 16). *About Us*. Retrieved September 16, 2009, from Census Bureau: http://2010.census.gov/2010census/

US Census Bureau. (2009, September 15). *Question & Answer Center*. Retrieved September 15, 2009, from U.S. Census Bureau: https://ask.census.gov/cgi-bin/askcensus.cfg/php/enduser/std_adp.php?p_faqid=709&p_created=1096559150&p_sid=HpRGZWHj&p_accessibility=0&p_redirect=&p_lva=&p_sp=cF9zcmNoPSZwX3NvcnRfYnk9JnBfZ3JpZHNvcnQ9JnBfcm93X2NudD0zNjg2LDM2ODYmcF9wcm9kcz0mcF9jYXRzPSZwX3B2

Vellani, K. a. (2001). *Applied Crime Analysis.* Woburn: Butterworth-Heinemann.

Vellani, K. (2006). Strategic Security Management. In K. Vellani, *Strategic Security Management* (pp. 12-13). Boston: Butterworth-Heinemann.

Woods, M. (1999, April). Crime Analysis: A Key Tool in Any Crime Reduction Strategy. *Police Chief* , pp. 17, 19-20, 22, 24, 28, 30.

Wortley, R. &. (2008). *Environmental Criminology and Crime Analysis.* Portland: Willan.

BIBLIOGRAPHY

Anselin, L., Cohen, J., Cook, D., Gorr, W. and Tita, G. (2000) 'Spatial Analysis of Crime', Measurement and Analysis of Crime and Justice 2000 (4): 213-262.

American Society for Industrial Security International (2003). *General security risk assessment.* Alexandria, VA: ASIS International.

Anselin, L., Cohen, J., Cook, D., Gorr, W. & Tita, G. (2000). Spatial Analysis of crime. In D. Duffee (Ed.*), Measurement and analysis of crime and justice, Criminal justice 2000, Vol. 4* (pp.213-262). Washington, DC: U.S. Department of Justice, National Institute of Justice.

Atlas, R. (2008). *21st century security and CPTED: Designing for critical infrastructure protection and crime prevention*. Boca Raton, FL: CRC Press.

Bates, Norman D (1997). "Foreseeability of Crime and Adequacy of Security", Accident Prevention Manual for Business & Industry, Security Management, National Safety Council.

Block, C.R., M. Dabdoub and S. Fregly (Eds), Crime Analysis Through Computer Mapping, Washington: Police Executive Research Forum: 111-128.

Boba, R. (2001). *Introductory guide to crime analysis and mapping.* Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Boba, R. (2003). *Problem analysis in policing*. Washington, DC: Police Foundation.

Brantingham, P.L. and Brantingham P. J. (1984) Patterns in Crime, New York: Macmillan Publishing Company.

Broder, J. F. (2006). *Risk analysis and the security survey.* 3rd ed. Boston: Butterworth-Heinemann.

Brotby, W. K. (2008). *Information security metrics: A definitive guide to effective security monitoring and measurement*. Boca Raton, FL: CRC Press.

Bruce, C.W., Hick, S.R., & Cooper, J. P. (2004). *Exploring crime analysis: Readings on essential skills.* Overland Park, KS: International Association of Crime Analysts.

Burrows, J. (1988). *Retail crime: Prevention through crime analysis*. (Crime Prevention Unit; Paper 11). London: Home Office.

Bynum, T. S. (2001). *Using analysis for problem-solving: A guidebook for law enforcement*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Carter, D. (2004*). Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Cavanagh, T. E. (2005). *Corporate security measures and practices: An overview of security management since 9/11*. New York: The Conference Board.

Cavanagh, T. E. (2006). *Navigating risk: The business case for security.* New York: The Conference Board.

Cavanagh, T. E. (2008). *Security metrics as a management tool.* (Executive Action Series; No. 268). New York: The Conference Board.

Chainey, S., Tompson, L., & Uhlig, S. (2008). The utility of hotspot mapping for predicting spatial patterns of crime. *Security Journal*, 21, 4-29.

Chapin, C., & Akridge, S. (2005). How can security be measured? *Information Systems Control Journal*, 2, 43-47.

Clarke, R. V., & Eck, J. (2005). *Crime analysis for problem solvers in 60 small steps.* Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Cope, N. (2004). Intelligence led policing or policing led intelligence? *British Journal of Criminology*, 44, 188-203.

DAddario, F. J. (1989). *Loss prevention through crime analysis*. Boston: Butterworths.

Eck, J. E. (2001). *Assessing responses to problems: An introductory guide for police problem solvers.* Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Eck, J. E., and LaVigne, N. (1994). *Using research: A primer for law enforcement managers.* 2nd ed. Washington, DC: Police Executive Research Forum.

Eck, J. E., & Weisburd, D. (Eds.) (1995). *Crime and Place.* (Crime Prevention Studies, Vol. 4) Monsey, NY: Criminal Justice Press.

Ekblom, P. (1986). *The prevention of shop theft: An approach through crime analysis.* London: Home Office.

Ekblom, P. (1988) Getting the Best Out of Crime Analysis, Crime Prevention Unit: Paper 10, London: Home Office.

Fay, J. J. (2006). *Contemporary security management.* 2nd ed. Boston: Elsevier Butterworth-Heinemann.

Federal Bureau of Investigation (2004). UCR Handbook. Washington, DC: U.S. Department of Justice.

Garcia, M. L. (2006). Risk management. In M. Gill (Ed.), *A handbook of security* (pp. 509-531). New York: Palgrave Macmillan.

Gebhardt, Christopher S. (1999). "Crime Analysis: The next phase." The Police Chief, April 1999.

Goldsmith, V., McGuire, P. G., Mollenkopf, J. H., & Ross, T. A. (Eds.) (2000). *Analyzing crime patterns: Frontiers of practice.* Thousand Oaks, CA: Sage.

Gottlieb, S., Arenberg, S., & Singh, R. (1998). *Crime analysis: From first report to final arrest*. Montclair, CA: Alpha Publishing.

Harries, K. (1999). *Mapping crime: Principle and practice.* Washington, DC: U. S. Department of Justice.

Jacquith, A. (2007). *Security metrics: Replacing fear, uncertainty, and doubt*. Upper Saddle River, NJ: Addison Wesley.

Jopeck, E. J. (2000). Five steps to risk reduction: Learn to identify and reduce risk by following these five steps. *Security Management*, 44(8), 97-98, 100-102.

Kitteringham, G. W. (2001). *A study of two types of vertical crime pattern analysis in the commercial multi-tenanted high-rise structure*. Leicester, UK: University of Leicester.

Kovacich, G. L., & Halibozek, E. P. (2006). *Security metrics management: How to manage the costs of an assets protection program*. Burlington, MA: Butterworth-Heinemann.

International Association of Crime Analysts (2004). Exploring Crime Analysis. Overland Park: International Association of Crime Analysts.

Lee, W. D. (2005). Risk assessments and future challenges. *FBI Law Enforcement Bulletin*, 74(7), 1-13.

Lersch, K. M. (2007). *Space, time, and crime.* 2nd ed. Durham, NC: Carolina Academic Press.

Liu, L., & Eck, J. (2008). *Artificial crime analysis systems: Using computer simulations and geographic information systems*. Hershey, PA: Information Science Reference.

Manning, P. K. (2008). *The technology of policing: Crime mapping, information technology, and the rationality of crime control*. New York: New York University Press.

Manunta, G. (2002). Risk and security: Are they compatible concepts? *Security Journal*, 15(2), 43-55.

McCue, C. (2003). Data mining and value-added analysis. *FBI Law Enforcement Bulletin*, 72(11), 1-6.

McCue, C. (2007). *Data mining and predictive analysis: Intelligence gathering and crime analysis.* Boston: Butterworth-Heinemann.

McCue, C., & Parker, A. (2003). Connecting the dots: Data mining and predictive analytics in law enforcement and intelligence analysis. *Police Chief,* 70(10), 125-126, 128.

McGuires, M. (2000). Policing by risks and targets: Some dimensions and implications of intelligence led crime control. *Policing and Society*, 9, 315-336.

Mena, J. (2003). *Investigative data mining for security and criminal detection.* Boston: Butterworth-Heinemann.

Miethe, T. D., & McCorkle, R. (1998). *Crime profiles: The anatomy of dangerous persons, places, and situations*. Los Angeles: Roxbury.

Osborne, D. A., & Wernicke, S. C. (2003). *Introduction to crime analysis: Basic resources for criminal justice practice.* Binghamton, NY: Haworth Press.

O'Shea, T., & Nicols, K. (2002). *Crime analysis in America: Findings and recommendations.* Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Pelfrey, W. V. (1992). Convergence of crime prevention, new policing approaches, and private security: Crime analysis. *Security Journal*, 3, 215-218.

Ratcliffe, J. H. (2007). *Integrated intelligence and crime analysis: Enhanced information management for law enforcement leaders*. Washington, DC: Police Foundation.

Ratcliffe, J. H. (2008). *Intelligence-led policing*. Cullompton, UK; Portland, OR: Willan.

Read, T., & Oldfield, D. (1995). *Local crime analysis.* (Crime Detection and Prevention Series: Paper No. 65). London: Home Office, Police Research Group.

Reuland, M. M. (1997). *Information management and crime analysis: Practitioners' recipes for success.* Washington, DC: Police Executive Research Forum.

Sennewald, C. A. (2006). *Effective security management*. 4th ed. Woburn, MA: Butterworth-Heinemann.

Sennewald, C. A., & Christman, J. H. (Eds). (2008). *Retail crime, security, and loss prevention: An encyclopedia reference.* Boston: Butterworth-Heinemann.

Sonnenreick, W., Albanese, J., & Stout, B. (2006). Return On Security Investment (ROSI): A practical quantitative model. *Journal of Research and Practice in Information Technology*, 38, 45-56.

Taylor, B., Kowalyk, A., & Boba, R. (2007). The integration of crime analysis into law enforcement agencies: An exploratory study into the perceptions of crime analysts. *Police Quarterly*, 10, 154-169.

Tilley, N. (2002). *Analysis for crime prevention.* (Crime Prevention Studies, Vol. 8). Monsey, NY: Criminal Justice Press.

U.S. Federal Bureau of Investigation (2008). *Crime in the U.S.: The uniform crime report*. Washington, DC: GPO, 2008.

U.S. Federal Bureau of Investigation (2004). *URC handbook*. Washington, DC: U.S. Department of Justice.

Vellani, Karim H. (2002). "Crime Analysis Literature: What We Have and Where We Are Going." Forecaster, International Association of Crime Analysts, Spring 2002.

Vellani, Karim H. (2006). "Crime Analysis" in John J. Fay's Encyclopedia of Security Management: Techniques and Technology, 2nd Edition. Woburn: Butterworth-Heinemann.

Vellani, K. H. (2007). *Strategic security management: A risk assessment guide for decision makers.* Boston: Butterworth-Heinemann.

Vellani, K. H., & Nahoun, J. (2001). *Applied crime analysis.* Boston: Butterworth-Heinemann.

Wang, F. (2005). *Geographic information systems and crime analysis*. Hershey, PA: Idea Group.

Weisburd, D., Bernasco, W., & Bruinsma, G. J. N. (Eds.) (2009). *Putting crime in its place: Units of analysis in geographic criminology.* New York: Springer.

Weisel, D. L. (2003). The sequence of analysis in solving problems. In J. Knutsson (Ed.), *Problem-oriented policing: From innovation to mainstream* (pp. 115-146). (Crime Prevention Studies, Vol. 15). Monsey, NY: Criminal Justice Press.

Woods, M. (1999). Crime Analysis: A Key Tool in Any Crime Reduction Strategy. *Police Chief*, 66(4), 17, 19-20, 22, 24, 28, 30.

Wortley, R., & Mazerolle, L. (Eds.) (2008). *Environmental criminology and crime analysis.* Cullumpton, UK; Portland, OR: Willan.

