Chapter 4

Crime Analysis

In this chapter . . .

- Statistics for Security Management
- Crime Triangle
- Purpose of Crime Analysis
- Data Sources
- Law Enforcement Data versus Social Disorder Models
- Advantages of Law Enforcement Data
- Geographic Levels
- Methodology
- Return on Security Investment

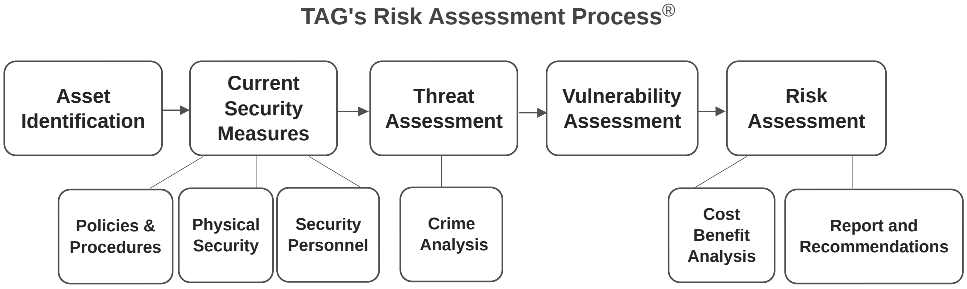


Figure 4-1.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

Statistics for Security Management

Statistics are used in planning for the future. As a key component of a threat assessment, crime and security statistics guide the risk assessment process, help in the selection of appropriate countermeasures, monitor program effectiveness, and alleviate risks and the associated costs of risks. The use of information regarding crimes and other security incidents helps the security decision maker plan, select, and implement appropriate security measures that address the actual risks of the facility. Security decision makers, after assessing the crime problem, can select the most effective countermeasures that eliminate risk or reduce it to an acceptable level. Budget justification is also accomplished through the use of statistics since effective security measures will reduce the risk, and returns on security investments can be calculated and considered in the bottom line.

A common application of statistics in the security arena is the use of security reports and crime data to determine the risks to a facility, including its assets and personnel. The security professional need not be a mathematician to fully utilize statistical data; rather, he or she needs only a basic understanding of the various methods to use such information, along with a basic knowledge of personal computer and spreadsheet software.

The use of statistics extends beyond planning security at an existing facility. Statistical data may also be used to select and plan security at new facilities. For example, the real estate department of an organization may provide the security decision maker with a list of potential new sites, one of which will be selected based on, among other things, the threats at the location. In this role, the security decision maker serves as an advisor to the real estate department by conducting crime analysis of the proposed sites as well as perform security surveys of each site to identify vulnerabilities in an effort to select the location that poses the least or a tolerable level of risk. In this scenario, the security decision maker will gather and analyze crime data for similar businesses in the area surrounding each site to determine the security problems. The sites that have the least number of crimes can be evaluated further by means of a security survey that identifies potential or existing vulnerabilities. After the sites have been narrowed down by threat and surveys have been completed, the security decision maker has the necessary information to advise the real estate department.

Integrating crime analysis into an existing risk model is a fairly simple task for most organizations. Threat assessment information is the backbone of security surveys and defines the scope of the security survey and vulnerability assessment. Before embarking on a security survey, security decision makers will have a thorough understanding of the threats, crimes, and security incidents at the facility. This information guides the security decision maker as he conducts the survey and looks for vulnerabilities and the crime opportunities that can be blocked with security measures.

For example, an office building security director concerned with a flood of thefts of employee wallets and purses may conduct a survey with an eye toward the opportunities that are available in the office suites. As he walks through the offices, he may find that purses and wallets are readily visible from office doors and windows, thus providing the opportunity for criminals to see the target property. A simple and cost-effective solution to this problem is to institute a "clean desk" policy whereby employees are encouraged to lock their personal belongings in their desks or a company locker.

A more serious security problem that the building security director may face is that of assaults and robberies in the parking garage adjacent to the office building. If the statistical information indicates that the assaults are occurring on the upper floors of the garage and the victim does not know the perpetrator, the security director will assess the security weaknesses of the parking garage. He may find that numerous unlit hiding areas provide the necessary cover for robbers. By applying relatively low-cost measures such as mirrors and lighting, the building security director will reduce the opportunity for criminals to hide.

> ***It isn't that they can't see the solution. It is that they can't see the problem.***
>
> ***—G.K. Chesterton from The Scandal of Father Brown***

Crime Triangle

Reducing the opportunity for crime to occur is a strategic goal of security professionals. Behind this goal is the concept of a crime triangle, whereby three elements must exist for a crime to occur:

Motive

Capability

Opportunity

With little or no control over a determined offender's desire, security decision makers focus their attention on the remaining elements of the crime triangle by attempting to block opportunities and remove motivation, both of which can be controlled to a large extent by an effective security program. Motivation is created by the actual crime target. In the private sector, a criminal's motive is the asset(s) that the security program is created to protect. Here again, assets include people, property, and information. Since organizations usually require assets to operate, the removal of motivation is a difficult task, if not altogether impossible. Most businesses must instead turn their attention to blocking the opportunity of crime. As seen in the Figures 4-2 and 4-3, blocking opportunities for crime leads to a reduction in crime.

The crime triangle is a simple, yet effective, method for illustrating how a crime can be prevented. More complex methods for explaining crime causation exist such as the Routine Activity theory developed by Marcus Felson. Part

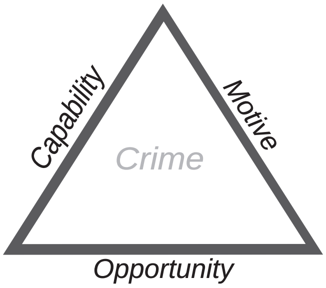


Figure 4-2.
Crime Triangle.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

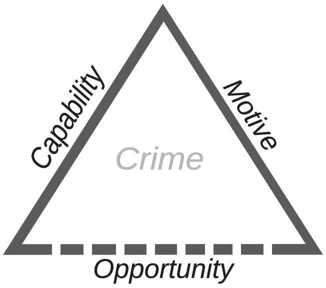


Figure 4-3.
Crime Triangle.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

of this theory explains crime causation and may be considered an expansion of the crime triangle. According to this explanation, for a crime to occur, six components must be present:

1. Motivated offender—a person ready and willing to commit a crime.
2. Absent or ineffective handler—a person who influences the behavior of the offender. Handlers include parents, relatives, friends, teachers, and employers.
3. Suitable target—a person or asset that is of value to an offender.
4. Absent or ineffective guardian—a person who protects the target from harm. Guardians include police, parents, relatives, friends, and property managers.
5. Time—a period for the first four ingredients to come together.
6. Space—a place for the first four ingredients to cross paths.

Purpose of Crime Analysis

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 founded. Whether one is working proactively to address security concerns or reactively in litigation or during the investigation of a crime, crime analysis is an effective tool. From an asset protection perspective, crime analysis is the identification of risk and vulnerability, and from a liability prevention perspective, crime analysis is the determination of foreseeability. Broadly speaking, crime analysis is the logical examination of crimes that 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 (*Applied Crime Analysis*, 2001).

While this definition of crime analysis is holistic, it can be dissected into three basic elements:

- The logical examination of crimes that 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
- The application of revised security standards and preventive measures

Examining crimes perpetrated at company facilities is commonplace in today’s business environment. In larger companies, a person or group of people may be 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 handled 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 workup or the tools to do so.

With regard to 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. (The various types of crime analysis methods are discussed in depth later in this chapter.)

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 is it 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 (spatial analysis), and when they occur (temporal analysis), among others. By using this information, it is much easier to select countermeasures aimed directly at the problem.

In summary, crime analysis seeks to:

- evaluate actual risk at a company's facilities and rank facilities by risk level.
- reduce crime on the property by aiding in the proper allocation of asset protection resources.
- justify security budgets.
- continually monitor the effectiveness of the security program.
- provide evidence of due diligence and reduce liability exposure.

Why would a security decision maker need to know how crime occurs? Understanding the factors that lead to crime, coupled with a comprehensive study of crime on the property, assists security decision makers in creating effective security programs to block opportunities for crime. Crime analysis seeks to answer the questions What? Where? When? Who?, How?, and Why?

Answers to these questions help security decision makers better understand the particular nature of crime on a given property and to formulate specific responses. The *What* question tells us what specifically occurred. For example, was the crime against a person or property, violent or not violent, 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 behind the site? If the incident occurred inside, did it occur in a public area or a controlled area? Determining the precise location assists security decision makers 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 gives us the temporal details of each incident. 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 in which a crime occurred.

Who answers several important questions that help a security decision maker 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 decision makers 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 decision maker's attention. For example, a residential apartment complex that caters to recently released psychiatric patients has a 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 whereby innkeepers were often found to be responsible for the safety of a guest when crime was foreseeable. People on travel usually do not know the area in which they are staying, and they also have little control over the security measures 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 of *How* the crime can be prevented in the future. More specific *How* questions may also be asked. For example, 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 immediately to 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 decision makers need to ask as many questions as possible about the criminal's actions to learn the most effective solutions. It is true that often the *How* question will be the most difficult one 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 because they have a perfectly valid reason for attending the location but in the course of their regular activities, they also carry out criminal activities.

External sources of crime are illegitimate users of the space whose prime motivation for coming to the site is to conduct some type of criminal activity. Security strategies may be vastly different between legitimate versus illegitimate users of space. For example, several barriers can exist between the outside public access and a specific target. If the property or security decision maker is only concerned with someone breaking into an area, then he or she will be ignoring the legitimate user who may have an access control card, Personal Identification Number, password, biometric feature, or any number of other avenues of entry.

With these answers, security professionals are better armed to attack the crime problem.

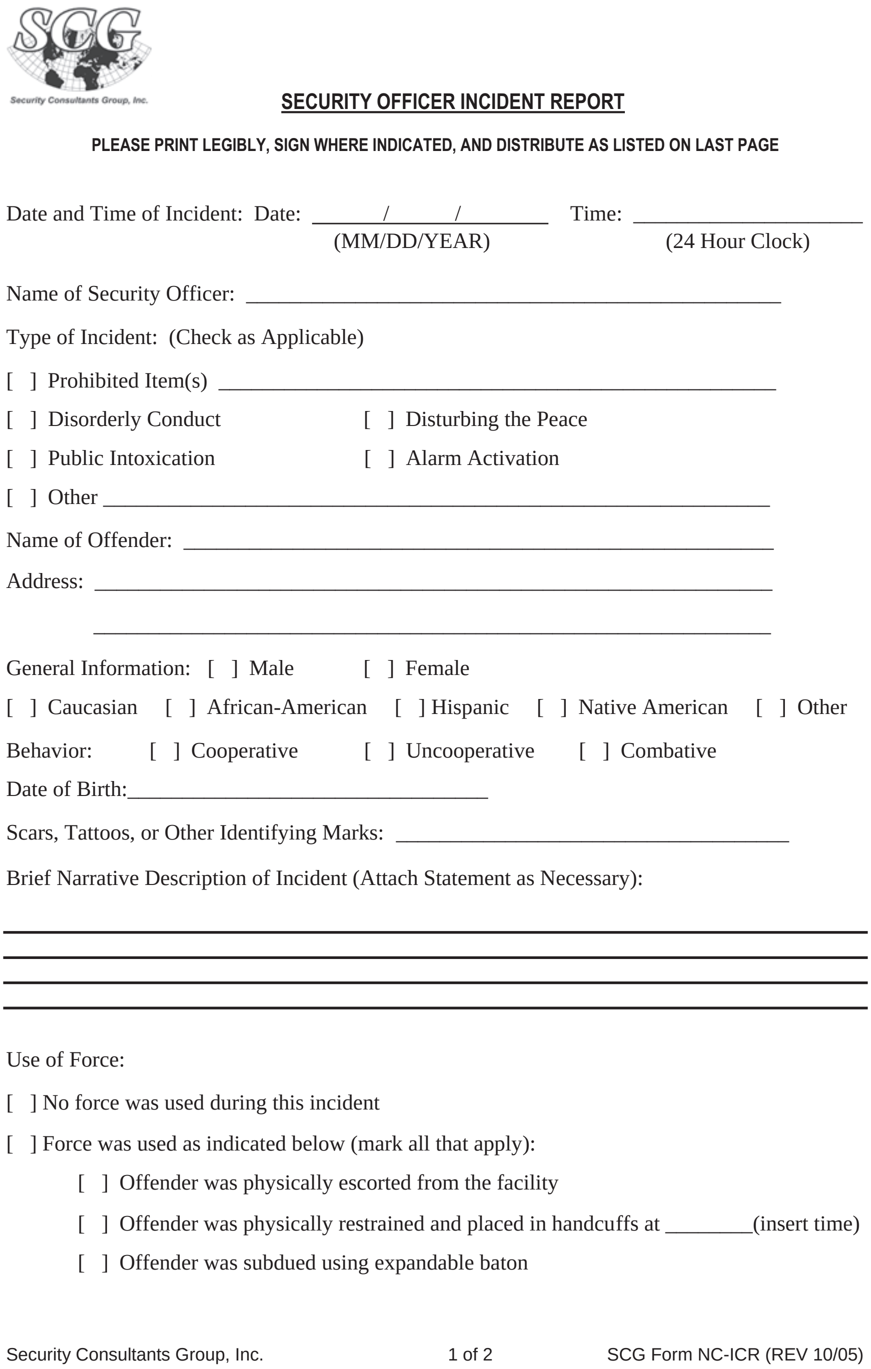
Data Sources

Security Reports

A valuable and highly encouraged source of data is the in-house security report (SR). As the name implies, SRs are reports of criminal activity and other incidents (parking, loitering, and security breaches) that may be of concern to security professionals. These reports may be generated by management directly or through contracted security companies. The validity of SR data is only as good as the policy that 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 SRs, management should be cautious not to exclude other sources of data and should not rely solely on in-house security reports. In requiring the collection of security reports, management can stipulate precisely what information is beneficial for their purposes and is contained within each report. Having said that, management should strive to include the following minimum 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 most successful use of security reports that the author has seen occurred in a large, multibuilding apartment community. After spending over $40,000 on fencing and access control systems to reduce the high level of auto thefts at the apartment complex, the apartment manager was distraught that the auto thefts continued at the complex despite the fact that the innovative access control system had been installed. As a consultant, the author was asked to analyze the situation and determine additional measures to be implemented to



SECURITY OFFICER INCIDENT REPORT

PLEASE PRINT LEGIBLY, SIGN WHERE INDICATED, AND DISTRIBUTE AS LISTED ON LAST PAGE

Date and Time of Incident: Date: ______/______/________ Time: ____________________
(MM/DD/YEAR) (24 Hour Clock)

Name of Security Officer: ____

Type of Incident: (Check as Applicable)

[ ] Prohibited Item(s) ____

[ ] Disorderly Conduct [ ] Disturbing the Peace

[ ] Public Intoxication [ ] Alarm Activation

[ ] Other ____

Name of Offender: ____

Address: ____

____

General Information: [ ] Male [ ] Female

[ ] Caucasian [ ] African-American [ ] Hispanic [ ] Native American [ ] Other

Behavior: [ ] Cooperative [ ] Uncooperative [ ] Combative

Date of Birth:______________________________

Scars, Tattoos, or Other Identifying Marks: __________________________________

Brief Narrative Description of Incident (Attach Statement as Necessary):

____

____

____

____

Use of Force:

[ ] No force was used during this incident

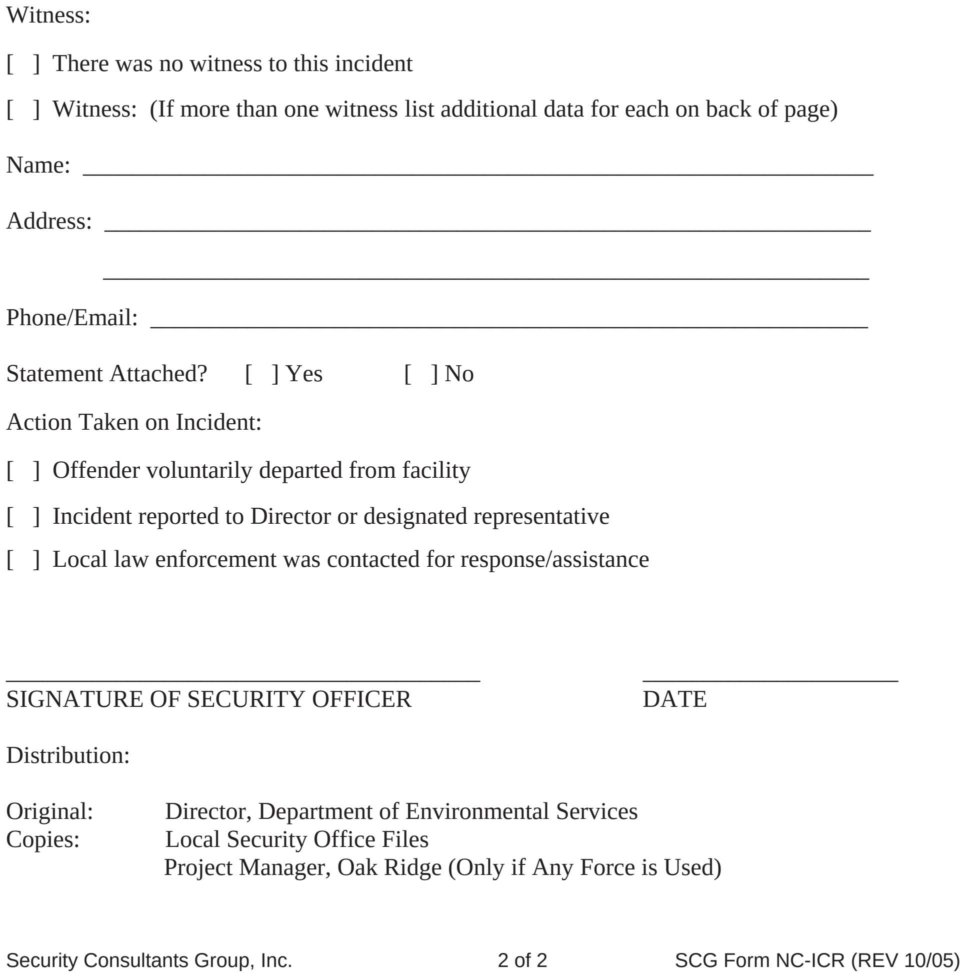
[ ] Force was used as indicated below (mark all that apply):

- [ ] Offender was physically escorted from the facility
- [ ] Offender was physically restrained and placed in handcuffs at ________(insert time)
- [ ] Offender was subdued using expandable baton

Security Consultants Group, Inc. 1 of 2 SCG Form NC-ICR (REV 10/05)

Figure 4-4.

Incident Report, Copyright ©2007 by Security Consultants Group, Inc. Used by permission. Additional information available from Security Consultants Group, Inc. via www.scgincorp.com.



Witness:

[ ] There was no witness to this incident

[ ] Witness: (If more than one witness list additional data for each on back of page)

Name: ____

Address: ____

____

Phone/Email: ____

Statement Attached? [ ] Yes [ ] No

Action Taken on Incident:

[ ] Offender voluntarily departed from facility

[ ] Incident reported to Director or designated representative

[ ] Local law enforcement was contacted for response/assistance

______________________________ ______________________

SIGNATURE OF SECURITY OFFICER DATE

Distribution:

Original: Director, Department of Environmental Services
Copies: Local Security Office Files
Project Manager, Oak Ridge (Only if Any Force is Used)

Security Consultants Group, Inc. 2 of 2 SCG Form NC-ICR (REV 10/05)

Figure 4-4.
Continued

thwart the problem. After analyzing the crime and verifying the extent of auto thefts, a review of the apartment's resident screening policies was conducted, and it was learned that management was not carrying out criminal background checks on prospective tenants as required by policy and leases.

The apartment management immediately conducted the checks and learned that three convicted auto thieves were living in one unit of the complex. This information was corroborated by analyzing the auto theft data for the complex which showed that, although auto thefts occurred in all areas of the parking lots, they were concentrated around the particular apartment building where the three men lived. Because the men lived on property, they had full, authorized access to the complex and its parking areas. Management proceeded to have the three men evicted for failing to pay their rent on time, and soon after the eviction was finalized the auto theft problem disappeared. This example shows the importance of following security policies and procedures as well as analyzing the crime statistics and other internal data thoroughly.

Law Enforcement Data versus Social Disorder Models

Some companies have used social disorder models in place of crime analysis, though more and more are realizing the problems associated with these models. Since the publication of *Applied Crime Analysis* in 2001, the author has seen more than 90 percent of his security consulting firm's clients migrate away from using social disorder theories toward utilizing true crime analysis. While those numbers are substantial, still many organizations do not understand the concerns of social disorder models, the most problematic of which are discussed here.

Social disorder models are based primarily on criminological theory with little practical use since the primary source of their metrics is demographic data. Among the primary problems of the social disorder model is the failure to publish the methodology used in arriving at the model's results. Without a published and peer-reviewed methodology, security professionals cannot rely on the data, and one can only imagine the implications of having a large part of a company's risk model rejected by the courts during litigation. Security directors have a responsibility to fully understand the risk model they use and to be prepared to explain it in deposition and trial when representing their company in litigation.

Another problem associated with social disorder models is their reliance on demographic data. Although private firms collect demographic data more frequently, the majority of demographic data in the United States is only collected every 10 years via the U.S. Bureau of the Census. Because of the time lag needed to obtain the demographic data and the subsequent time required to develop the model from that data, results are not timely. Social disorder models also present some challenges in effectively removing race from the analysis since the base demographic data are based on an area's population and its characteristics, including socioeconomic levels, education levels, and personal traits of the populace such as age, sex, and race. Contrary to FBI crime reports and actual police data, large areas of the United States are considered high crime according to social disorder models, necessitating many companies to discontinue use of the model in large parts of the country. Some companies have faced charges of redlining, which is the private-sector equivalent of racial profiling, resulting in a negative impact on the corporate reputation.

Advantages of Law Enforcement Data

Police data represents the most widely used source data for crime analysis because it presents an accurate crime history for a property and is from an objective source. Since police departments don't have a stake in a company or any associated liability exposure, their crime data is considered reliable and unbiased. Although some instances of city or county-wide crime statistics manipulation have occurred historically in some law enforcement jurisdictions, rarely, if ever, are the statistics for specific addresses and facilities skewed. Most crime data manipulation occurs to overall city crime levels to serve various political goals. At the facility level, law enforcement agencies have little reason to skew the statistics.

Another advantage of police crime data is its vast availability due to extensive reporting, capturing, and maintenance of the crime statistics across most jurisdictions in the United States. Although costs for the data vary from jurisdiction to jurisdiction, most fees are reasonable. The only downside to police data is the time required to obtain it from police agencies, with the necessary time ranging from hours to weeks.

Various crime data and analysis methodologies have been published and used by many cutting-edge companies in the protection of assets. Crime analysis methodologies have been published and subjected to peer review in various security and police textbooks, the definitive security book being *Applied Crime Analysis*.

Law enforcement data is almost always accepted by the courts and in fact is sometimes required by the courts in determining the foreseeability of crime. Although a particular methodology may be subjected to scrutiny, the data is normally admissible. The security professional tasked with testifying on behalf of his or her employer is safe to rely on crime data from police departments as long as the methodology used is sound.

Law Enforcement Data Sources

Among law enforcement data sources are Uniform Crime Reports (UCR), Calls for Service (CFS), and Offense Reports. These data sets are typically easy to obtain, and in the case of UCR for large geographic areas, they are available online at the Federal Bureau of Investigation website (www.fbi.gov). Local law enforcement data is normally accessible via Freedom of Information (FOIL) requests or under individual state laws regarding public information. For state laws and detailed instructions, contact the state's Office of the Attorney General.

Uniform Crime Reports

According to the Federal Bureau of Investigation, "the Uniform Crime Reporting Program was conceived in 1929 by the International Association of Chiefs of Police to meet a need for reliable, uniform crime statistics for the nation. In 1930, the FBI was tasked with collecting, publishing, and archiving those statistics. Today, several annual statistical publications, such as the comprehensive *Crime in the United States*, are produced from data provided by nearly 17,000 law enforcement agencies across the United States. *Crime in the*

United States (CIUS) is an annual publication in which the FBI compiles the volume and rate of crime offenses for the nation, the states, and individual agencies. This report also includes arrest, clearance, and law enforcement employee data."

The Uniform Crime Report, or UCR as it is commonly known, is the nation's crime measure. It employs constant crime definitions across the country's many law enforcement jurisdictions and measures the following crimes:

Part I Offenses

1. Murder
2. Rape
3. Robbery
4. Aggravated Assault
5. Burglary
6. Theft
7. Motor Vehicle Theft
8. Arson

Part II 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

These crimes were selected because they are serious, they occur frequently, they are likely to be reported to law enforcement, they can be confirmed by means of investigation, and they occur across all jurisdictions in the country. Developed by the FBI, the UCR includes crime data for most geographic areas in the United States ranging from counties and cities to the nation as a whole. Intermediate areas, such as state and metropolitan statistical area (MSA) crime data, are also available. Although these areas are too large to be included as the primary focus of crime analysis, the methodology and classification system is what security professionals should understand and use at the property level.

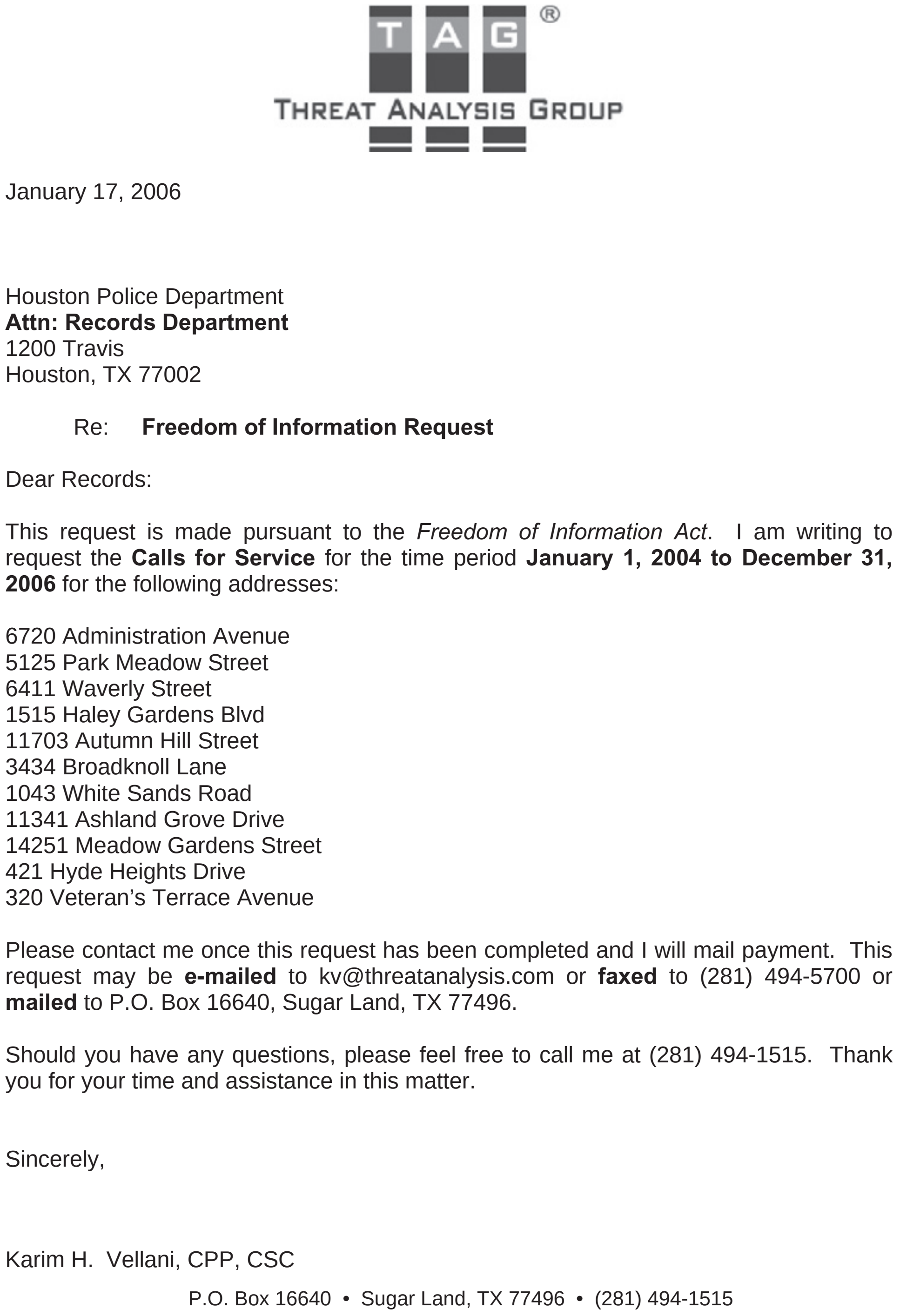
When using the UCR, it is best to examine violent and property crimes separately because they pose different concerns for security professionals and may require the application of different security measures. To be certain, crimes should be evaluated individually and as specifically as possible. For example, the crime of robbery can be further divided into robbery of a business and robbery of an individual. Often, the security measures used to counteract these two robbery types are different.

Calls for Service (CFS)

Although internal security reports and police crime data may overlap, it is incumbent upon the security decision maker to consider both in determining a facility's true risk. Thus, the next step is to contact the local police department and determine what types of data are available by address. Though it is rare, UCR data or actual crime information can sometimes be obtained for a specific address. If it is available, it should be requested and analyzed (see UCR above). If UCR data by address is not available, Calls for Service (or 911 dispatch logs as they are referred to in some departments) should be requested from the law enforcement agency.

The primary data set is Calls for Service (CFS), which serves as the basis for crime analysis and provides for the most accurate portrayal of criminal and other activity at a property. CFS may be regarded as the complete array of fragments that, when joined, form the most strikingly grounded survey of criminal activity for a specific property. Calls for Service consists of every report of crime, suspected crime, and activity called in to the police from a property. No other crime information source is as focused on a specific address for such a vast time span as Calls for Service, with the possible exception of in-house security reports generated by personnel operating on property 24 hours a day, 7 days a week. These inclusions, by definition, omit the imprecise factor of unreported crime. Research has concluded that unreported crime accounts for a 10 percent higher crime index, although this is highly dependent on the type of crime under observation. Despite the exclusion of unreported crime, Calls for Service still provides representative illustrations of criminal activity on a property.

Calls for Service consists of those crimes or other activity reported by a victim, witness, or other person to a local law enforcement agency via the 911 emergency system and other channels. These reports may consist of actual crimes ranging from murder to theft, or suspicious activity, and other incidents



TAG®
THREAT ANALYSIS GROUP

January 17, 2006

Houston Police Department
Attn: Records Department
1200 Travis
Houston, TX 77002

Re: **Freedom of Information Request**

Dear Records:

This request is made pursuant to the *Freedom of Information Act*. I am writing to request the **Calls for Service** for the time period **January 1, 2004 to December 31, 2006** for the following addresses:

6720 Administration Avenue
5125 Park Meadow Street
6411 Waverly Street
1515 Haley Gardens Blvd
11703 Autumn Hill Street
3434 Broadknoll Lane
1043 White Sands Road
11341 Ashland Grove Drive
14251 Meadow Gardens Street
421 Hyde Heights Drive
320 Veteran's Terrace Avenue

Please contact me once this request has been completed and I will mail payment. This request may be **e-mailed** to kv@threatanalysis.com or **faxed** to (281) 494-5700 or **mailed** to P.O. Box 16640, Sugar Land, TX 77496.

Should you have any questions, please feel free to call me at (281) 494-1515. Thank you for your time and assistance in this matter.

Sincerely,

Karim H. Vellani, CPP, CSC

P.O. Box 16640 • Sugar Land, TX 77496 • (281) 494-1515

Figure 4-5.
Sample Request Letter for Calls for Service.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

such as missing children, motor vehicle accidents, and parking complaints. Whatever the concern, if it is reported by a person, it is noted by the law enforcement agency. The synopsis of the given incidents is included on the record, along with the location, date, and time the event was reported. From devastatingly influential to seemingly insignificant, these records exist as clues waiting to be examined in some Holmesian mystery and because of their completeness of representation and maintenance by a local governing body, and as they operate independent from the security decision maker's interests, they can generally be considered objective, thus adding the first of many threads of reliability to the crime analysis conclusions. In addition to the more obvious crimes, CFS adds elements that may be of interest to management such as the above-mentioned suspicious activity, accidents, and parking violations that could be realized to be important in the holistic concept of crime prevention.

Being hyperinclusive, no single set of data exists that rivals Calls for Service for its accuracy. As with any set of statistics, many more desirable possibilities can be derived by performing additional correlations such as sorting crimes by precise location on the property and by times at which they occurred. When more raw data is available in one's database, more meaningful cross-references and correlations are possible. One can consider that some of the fundamental ways people learn about various disciplines is through comparison, trial and error, or cause-and-effect methods. CFS allows trends or patterns in crime activity to come to light, which aids in the selection of appropriate crime countermeasures and provides for more enlightened comparisons between properties.

Among other considerations that users of CFS should remember, CFS data reflects 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 can be enhanced when CFS is used in conjunction with the local law enforcement agency's offense or incident reports (which will be discussed in depth later in this chapter).

Some newer CFS systems encode data using the FBI'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, however, must be converted to UCR through verification with offense reports.

CFS is generally available from the local police department at a reasonable cost. In light of the availability and aforementioned considerations, CFS data can be used effectively to produce a fairly accurate crime history of a property, distinguish any crime trends or patterns, and compare properties.

Reliability of Calls for Service (CFS)

The reliability of CFS has been tested to meet the demands of forecasting crime and other activity that might be of interest to management; among these activities are minor or major traffic accidents, medical emergencies, parking problems, and essentially any situation that may possibly present concerns that would occupy the time of security decision makers to solve or remediate. One study indicates that Calls for Service over a year's period would have a 90 percent accuracy rate—significantly higher than demographic data in predicting crime in the long run.

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

Reliability of CFS data in predicting long-run risks (all calls, not just crimes):

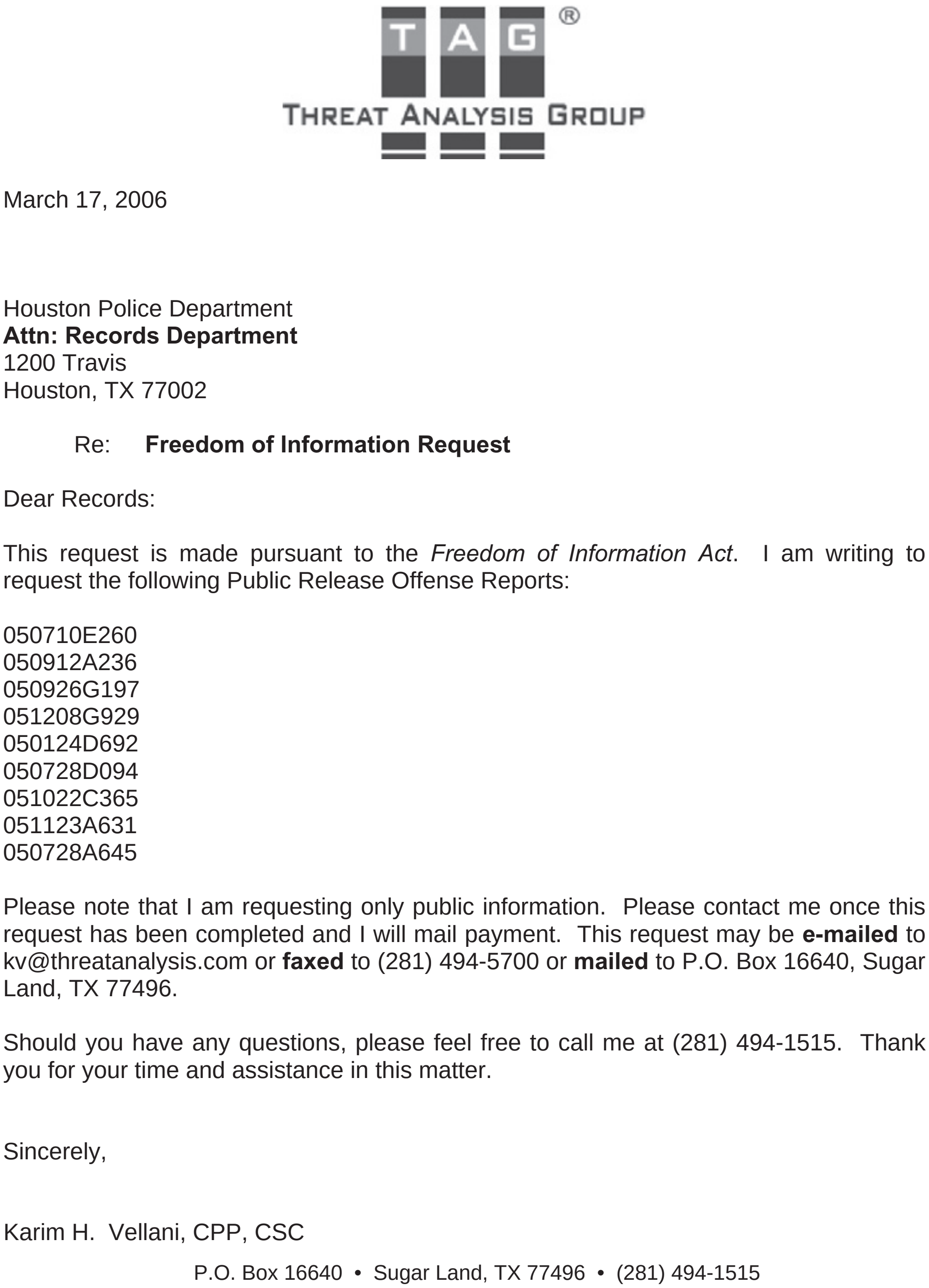
One month of data = 50% accuracy
Two months of data = 60–65% accuracy
Six months = 80%
1 year (13 28-day periods) = 90%

Source: Spelman in *Crime and Place*, 135

Offense Reports

Offense reports are the written narrative of a crime investigation and are used to verify CFS. This verification process is necessary because, as noted earlier, 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, the public information section contains enough information to allow an accurate database of crime incidents. Generally speaking, crime analysis seeks to build the most accurate database possible using only public information. During the course of a lawsuit, complete offense reports including arrest records and final case dispositions become available by subpoena, but the goal here is to proactively address the crime situation to prevent injuries and lawsuits.

More of an expansion of Calls for Service than an independent data source, offense reports, or incident reports as they are sometimes known, should clear up ambiguities and possible inaccuracies through verification of CFS. Sometimes, however, an offense report is generated when police officers discover a crime independent from a call into the 911 emergency system. More precisely, offense reports are the written narrative of a Call for Service that resulted in



TAG®
THREAT ANALYSIS GROUP

March 17, 2006

Houston Police Department
Attn: Records Department
1200 Travis
Houston, TX 77002

Re: **Freedom of Information Request**

Dear Records:

This request is made pursuant to the *Freedom of Information Act*. I am writing to request the following Public Release Offense Reports:

050710E260
050912A236
050926G197
051208G929
050124D692
050728D094
051022C365
051123A631
050728A645

Please note that I am requesting only public information. Please contact me once this request has been completed and I will mail payment. This request may be **e-mailed** to kv@threatanalysis.com or **faxed** to (281) 494-5700 or **mailed** to P.O. Box 16640, Sugar Land, TX 77496.

Should you have any questions, please feel free to call me at (281) 494-1515. Thank you for your time and assistance in this matter.

Sincerely,

Karim H. Vellani, CPP, CSC

P.O. Box 16640 • Sugar Land, TX 77496 • (281) 494-1515

Figure 4-6.
Sample Request Letter for OR's.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

an actual crime and includes the individual reports of all law enforcement agents, including officers, detectives, and supervisors who worked the case.

Although the availability of offense reports may be limited by law because of inclusion of personal information, victim names, criminal methods, or ongoing investigation, security decision makers should attempt to obtain them from the local law enforcement agency while in the process of conducting crime analysis. Often, however, most states allow the report or a portion of the narrative to be released to the general public upon request. As with all information, security decision makers should seek access to as much relevant crime information as possible to help them make knowledgeable management decisions. By no means should security decision makers feel that they are in error for not including offense reports when they are not available; on the contrary, one can only do what is reasonable and possible.

Geographic Levels

Before delving into the crime analysis methodology, it is imperative to determine what geographic area is to be covered by the crime analysis. For the purpose of crime analysis, a hierarchy defines the geographic levels of analysis. Although one cannot mathematically quantify the importance of each level of geographic analysis, one can distinguish a relationship between each level, or ascertain the order of importance for each level. In defining each level, they have been listed in order of importance, and simultaneously in the order that should be of most concern.

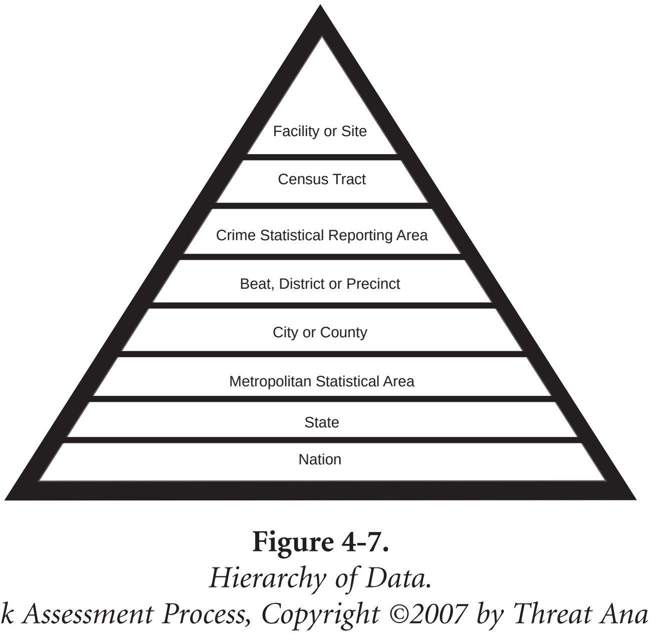

Facility or Site
Census Tract
Crime Statistical Reporting Area
Beat, District or Precinct
City or County
Metropolitan Statistical Area
State
Nation

Figure 4-7.
Hierarchy of Data.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

Facility or Site

From a security professional's perspective, control of crime is normally limited to the organization's facilities. This geographic area is the fundamental level of analysis for both crime prevention and liability prevention inasmuch as security personnel have the greatest ability to regulate most facets of its use. The primary sources of crime data for this level are CFS and offense reports, as well as in-house security reports, if they are available. Although security may influence neighboring areas with a diffusion of benefits—a process by which security measures implemented at one property may prevent crime at another location—the goal is to prevent crime at the controlled facility. For example, a security decision maker may be able to reduce crime on neighboring properties by increasing the lighting on his or her property as the light cannot be wholly contained to one property. Thus, security measures may positively impact neighboring properties indirectly.

As we move away from the property level in the crime analysis, the geographic areas get larger and less easily influenced. The smaller areas that can be analyzed include Census Tract, Crime Statistical Reporting Areas, and Beats, Districts, or Precincts. Police departments sometimes maintain crime data for these areas. Although they are only marginally useful in crime analysis, they do assist us in determining how our area compares to other areas in the same city. Whenever possible, the population should also be known for these areas so that the crime rate may be calculated (see Methodology below).

Census Tract

Census tracts are geographic areas defined by the U.S. Census Bureau for population and demographic purposes. In some instances, law enforcement agencies accumulate crime statistics by census tract. Since this occurs infrequently, it is not a standard level of crime analysis, but it may be included if the local law enforcement agency maintains data by census tract.

Crime Statistical Reporting Area

A reporting area (RA) is another uncommon level of analysis and criteria, for their creation may diverge significantly across law enforcement jurisdictions. Generally, RAs are small, homogeneous areas created for the sole purpose of supporting crime data collection. When RA data is available, it may be used to assist with the crime analysis of an individual property.

Beat, District, or Precinct

Patrol beats are common geographic zones in metropolitan areas that are created by law enforcement agencies to meet their resource allocation objectives—the number of patrol units in an area (beat). Beats are sometimes grouped together and fall under one command center, district, or precinct. The actual land area of beats, the total number of beats, and the number of districts/precincts overseeing the beats can vary considerably in different cities. Crime data for these areas is normally available from the local law enforcement agencies on an annual basis and often maintain crimes similar to those in the Uniform Crime Report.

Larger areas may also be considered in the crime analysis. These areas include cities and counties, states, metropolitan statistical areas, and the nation, and they are all included in the UCR. The advantage to these geographic areas is that population data is available; however, their sheer size creates a disadvantage.

City/County

City and county crime data is available from the Uniform Crime Report and encompasses crime information for an entire law enforcement jurisdiction. County data includes only the crime statistics for rural (unincorporated) areas and not the information for cities within the county.

Metropolitan Statistical Area (MSA)

Another geographic area created purely for crime statistical purposes, metropolitan statistical areas account for approximately 76 percent of the total U.S. population. MSAs consist of core cities of over 50,000 people and the surrounding suburban regions.

State

Similar to city and county data, state data can be found in the Uniform Crime Report and includes crime information for the entire state. This level of analysis details crime statistics for individual states and is often available from a state law enforcement agency.

Nation

Crime statistics for the nation are primarily available through the Uniform Crime Report program, via actual crime information and estimations for the occasional law enforcement jurisdictions that are not involved in the program. While larger geographic areas are easier to analyze owing in large part to the availability of crime statistics, crime at each facility tells the more accurate story.

Methodology

The best method for learning the true risk at a facility is to analyze internal security reports and verified police data using a computer spreadsheet application or database software program. Once this information is in a usable format, a number of basic and advanced statistical analyses can be performed. The security decision maker will adapt the analysis to best meet the needs of his or her organization. Whereas some security professionals prefer highly detailed charting and graphing functions, others prefer to view the raw numbers. Either way is fine as long as the security professional is comfortable and able to disseminate the information to those who need the data. Among the statistical tools available to the security decision maker are crime-specific analysis, modus operandi analysis, crime rate ranking, forecasting, temporal analysis, spatial analysis, and pattern analysis.

The crime analysis methodology outlined below has been tested in the courts and in private organizations, is based on a logical foundation, and provides useful information for a security decision maker. By no means is the methodology limited to what is described, for security professionals may for the most part find that the information requires customization to meet company needs. Whatever the case, this methodology provides the cornerstone from which a more comprehensive analysis can be built when necessary.

Whatever methodology is utilized in crime analysis, it should at minimum coincide with case law on issues of foreseeability so that claims of negligent security can be negated. Most states use crime data to determine if crime was foreseeable (predictable) and if management is on notice of crime. If management is found to be on notice of crime in the area or on the property, they normally have a duty to protect their invitees (customers, employees, etc.) against it. Although a foreseeability analysis is a good place to start the process of crime analysis, it certainly need not be the end. To be proactive, security decision makers require more data analysis in order to efficiently track security deficiencies and deploy more effective security measures.

Courts have typically accepted two to five years of historical crime data in premises liability lawsuits, while for security purposes, recommending three years of crime data. At this point, the Calls for Service and corresponding offense reports should have been requested and received from the law enforcement agencies and in-house security reports will have been incorporated into the database or spreadsheet application. Altough crime analysis can be conducted using paper and pen, software applications are recommended as they permit quicker data entry, sorting, and analysis of the data. Software application also allows users to easily create graphs, charts, and maps. A typical spreadsheet will start with keying in basic elements 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 it is not listed on the offense report.
- Offense Report (or Incident) Number—This is 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 was internally or externally generated.

Since most law enforcement agencies use different offense report forms, at first it may be difficult to ascertain each of the elements that are to be included in the database. However, given some practice with each law enforcement agency's forms, the process becomes rather routine. Once all the information from the offense reports has been entered, security report information can be added, with caution taken not to duplicate entries from the offense reports. Additional codes may be created for incidents of concern to management that are not included in the UCR coding system. The crime analysis format should be versatile and expandable so that when new data becomes available or when management needs change, different types of analysis may be added.

Once the data, including Calls for service, offense reports, and in-house security reports for the property has been assembled, it needs to be translated into a standardized set of codes that denote actual crimes. To ease comparisons, the UCR codification system should be used because it is simplistic and other data sets already use it. If anything other than UCR codes are provided, then the crimes must be transferred to UCR codes. This is required because police reports may differ in how they are worded or coded from the norm or from one another; to simplify matters, the UCR coding system is recommended because it includes a fairly complete listing of possible crimes, which will make analysis that much more complete.

Using this main database, security decision makers can sort information by site, by type of crime, and by date, time, or day of week. The database will also allow the security decision maker 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).

Another piece of data that should be entered on the spreadsheet is the site's annual traffic level, which is generated from internal records. The traffic level will be used as the site's population to calculate crime rates and trends. Traffic levels may also be calculated using transaction counts or other data that reflects the number of persons at a property. For example, at an apartment complex, they may use two residents per one-bedroom apartment unit and three residents per two-bedroom apartment unit. Thus, for a 100-unit apartment building that has 50 two-bedroom units and 50 one-bedroom units, the population of the apartment building would be 250 people:

$$\begin{aligned} 2 \text{ people} \times 50 \text{ one bedroom units} &= 100 \text{ people} \\ + 3 \text{ people} \times 50 \text{ two bedroom units} &= 150 \text{ people} \\ &= 250 \text{ people.} \end{aligned}$$

Most security decision makers would add other people who are frequently on premises, including employees such as maintenance and leasing personnel.

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.

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

Several different types of analysis make up a crime analysis as a whole. These include Temporal Analysis, Crime-Specific Analysis, Crime Rate Analysis, Spatial Analysis, Modus Operandi Analysis, and Forecasting. Each of these modes of analysis examines an aspect of crime's impact at a facility, identifies crime patterns and trends, and indirectly points to security measures that are appropriate to counter the known risks.

Crime-Specific Analysis

Although the FBI's UCR coding system breaks crimes down into their specific legal elements, it is often beneficial to break crimes down into sublevels for security purposes. Crime-specific analysis focuses not only on the type of crimes committed at a facility by enumerating the amount of crimes such as robberies and assaults, but also on whether the robbery victim was a business or an individual. Further specificity aids management in knowing the specific type of problem, to what degree it exists, and indirectly what specific crime prevention measures can be used to reduce the opportunity for those problems, if not eradicate them completely. 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 with 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.

Crime Rate Analysis

Crime rates, like most statistics, exist to actively represent events that have transpired or to extend that number to forecast future occurrences. Within crime analysis, crime rates assess a property's risk of violent and property crime victimization. The calculation of crime rate is fairly uncomplicated and requires little more than two pieces of data—a management-derived figure and a figure gleaned from the crime statistics. Simply stated, the violent crime rate is calculated by dividing the number of crimes by the traffic level and then multiplying by 1,000—the number commonly used to compare crime rates across the various levels of geographic analysis. In contrast, for property crime rates, the number of property targets is used 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. Crime rates should be calculated using the number of targets as the denominator. In other words, for crimes against persons, the denominator should be the number of persons. For crimes against properties, the denominator should be the number of items under consideration.

Crime rates are one of the best methods for comparing crime at various facilities. They should be used whenever possible because they offer the most accurate reflection of crime at a site by taking not only the crime level into account, but also the traffic level. By utilizing the population and transaction counts discussed above, a security decision maker is able to make apples-to-apples comparisons of facilities under his or her control to similar businesses in the area, as well as to larger geographic areas such as the city in which the facility is situated. Comparisons may also be made to other geographic areas for which crime statistics are available including census tracts, police beats, MSAs, states, and the nation as a whole. Again, 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.

Crime rates are calculated using the following formula:

$$\text{Violent Crime Rate (VCR)} = (\text{Total Violent Crime/Population}) \times 1{,}000$$

Table 4-1

Spreadsheet with Victim, Location, Comment.

Offense Report #	Site ID	Crime Type ID	Crime Type	Date	Time	Location	Victim	Comments
2004-00568	10	1	Murder	Tuesday, July 27, 2004	8:06	Outside	Person	Aggravated Robbery
2004-00001	70	2	Rape	Thursday, January 01, 2004	8:00	Outside	Person	Interpersonal
2005-05795	10	2	Rape	Tuesday, July 12, 2005	23:58	Outside	Person	Interpersonal
2004-00025	90	3	Robbery	Wednesday, January 07, 2004	7:07	Outside	Person	Aggravated Robbery
2004-00193	20	3	Robbery	Wednesday, March 10, 2004	9:32	Outside	Person	Aggravated Robbery
2005-00027	70	3	Robbery	Sunday, January 23, 2005	15:25	Outside	Person	Aggravated Robbery
2005-00110	10	3	Robbery	Thursday, March 24, 2005	22:51	Outside	Person	Aggravated Robbery
2005-00234	70	3	Robbery	Tuesday, July 12, 2005	14:18	Outside	Person	Aggravated Robbery
2005-00464	20	3	Robbery	Friday, October 28, 2005	15:59	Outside	Person	Aggravated Robbery
2005-00531	10	3	Robbery	Friday, December 09, 2005	5:34	Outside	Person	Aggravated Robbery
2004-00095	10	3	Robbery	Wednesday, February 04, 2004	22:00	Outside	Person	Car Jacking
2004-00356	50	3	Robbery	Monday, May 10, 2004	19:14	Outside	Person	Car Jacking
2004-00457	40	3	Robbery	Sunday, June 20, 2004	16:45	Outside	Person	Car Jacking
2004-00862	50	3	Robbery	Tuesday, December 07, 2004	14:08	Inside	Business	Car Jacking
2005-00253	50	3	Robbery	Friday, July 22, 2005	19:07	Outside	Business	Car Jacking
2005-00317	40	3	Robbery	Friday, August 26, 2005	15:24	Inside	Person	Car Jacking
2005-00360	20	3	Robbery	Thursday, September 22, 2005	20:35	Outside	Person	Car Jacking
2005-00407	90	3	Robbery	Friday, October 07, 2005	7:23	Outside	Person	Car Jacking
2004-00630	60	3	Robbery	Friday, August 20, 2004	10:00	Outside	Person	Interpersonal
2004-00089	20	3	Robbery	Sunday, February 01, 2004	4:45	Outside	Person	Purse Snatching
2004-00168	10	3	Robbery	Sunday, March 07, 2004	12:22	Outside	Person	Purse Snatching
2004-00371	90	3	Robbery	Tuesday, May 18, 2004	22:00	Outside	Person	Purse Snatching
2004-00442	30	3	Robbery	Sunday, June 13, 2004	20:05	Outside	Person	Purse Snatching
2004-00494	80	3	Robbery	Tuesday, July 06, 2004	7:07	Outside	Person	Purse Snatching
2004-00726	50	3	Robbery	Wednesday, September 29, 2004	19:05	Outside	Person	Purse Snatching
2004-00729	10	3	Robbery	Saturday, October 02, 2004	0:30	Outside	Person	Purse Snatching
2004-00756	70	3	Robbery	Monday, October 18, 2004	8:28	Outside	Person	Purse Snatching
2004-00811	20	3	Robbery	Friday, November 12, 2004	12:05	Outside	Person	Purse Snatching
2004-00905	30	3	Robbery	Tuesday, December 21, 2004	9:32	Outside	Person	Purse Snatching
2005-00045	40	3	Robbery	Sunday, February 06, 2005	16:44	Outside	Person	Purse Snatching
2005-00112	60	3	Robbery	Thursday, March 24, 2005	14:16	Outside	Person	Purse Snatching
2005-00158	80	3	Robbery	Friday, April 29, 2005	18:41	Outside	Person	Purse Snatching
2005-00236	40	3	Robbery	Thursday, July 14, 2005	17:00	Outside	Person	Purse Snatching
2005-00361	10	3	Robbery	Thursday, September 22, 2005	10:00	Outside	Person	Purse Snatching
2005-00512	10	3	Robbery	Wednesday, November 30, 2005	9:32	Outside	Person	Purse Snatching
2005-00552	70	3	Robbery	Monday, December 19, 2005	23:17	Outside	Person	Purse Snatching

Note that the crime rate refers to violent crimes, which have an easily countable target via the site's traffic level (population). Other crimes, such as auto theft, will have calculable crime rates if the target count is available. For example, the auto theft crime rate can be figured using the auto theft level and the annual number of vehicles on the property (traffic level). Thus, with 17 auto thefts and an average of 3,500 cars per day last year, our auto theft rate is 4.86 per 1,000 autos:

Auto Theft Rate = (Total Auto Theft/Population) × 1,000
Auto Theft Rate = (17/3,500) × 1,000
Auto Theft Rate = (0.00486) × 1,000
Auto Theft Rate = 4.86

Using this formula for each site allows us to accurately compare risk levels at different sites. This formula may be applied to each year of the crime analysis to formulate trends and patterns over time, which are easily discernible when graphed. Burglary rates are calculated by dividing the number of burglary events by the number of targets. In a large apartment community with 2,000 units and 5,000 residents, the appropriate denominator for calculating the property crime rate is 2,000, while the denominator for calculating the violent crime rate is 5,000. Taking this example further, if the community experienced 25 violent crimes and 200 property crimes during the preceding year, the violent crime rate is 0.005 [(25/5,000)*1,000], while the property crime rate is 100 [(200/2,000)*1,000]. Simply stated, for crimes against persons, the denominator should be the number of persons. For crimes against properties, the denominator should be the number of properties.

Temporal Analysis

Various methods for understanding a facility's crime peaks and valleys are available to the security manager. Temporal analysis, or the analysis of time, is among the most effective tools for allocating security resources. Patterns can be considered, including time of day, day of week, week of month, seasonal trends, and, at the extreme, crime trends during full moons. If there is historical evidence that particular crimes occur during certain periods, security can focus on additional crime defense measures during those time periods. Deploying security measures during periods of high crimes can save the security department money and generate cost avoidances that can be used in calculating Return on Investment.

Temporal analysis is the consideration of time periods when crimes occur. It allows the security decision maker to effectively allocate scarce security resources during peak crime periods. Although other security practices can be adjusted and modified based on temporal analysis, its most common use is in the efficient scheduling of security and protective force personnel.

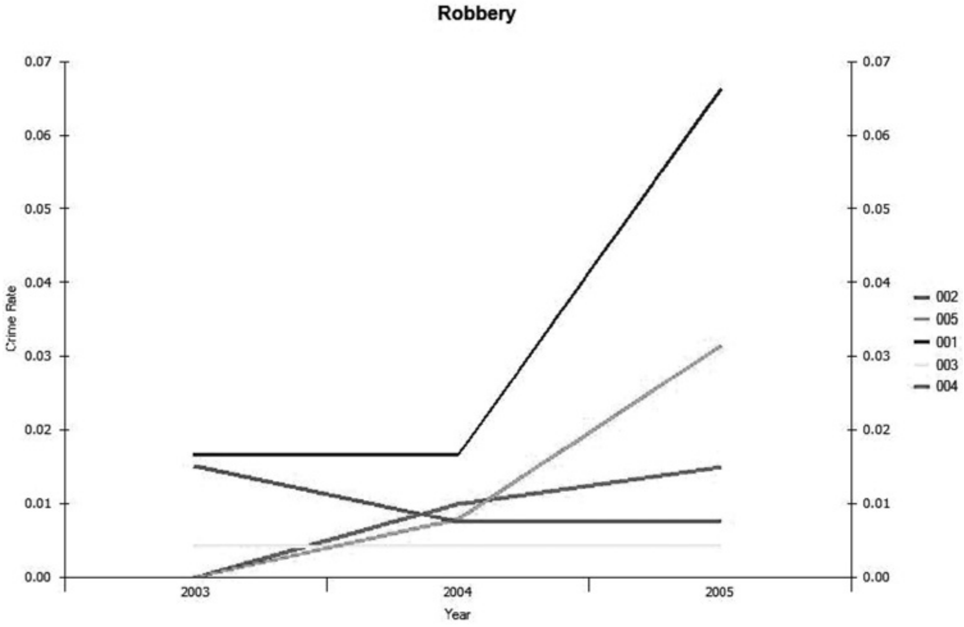
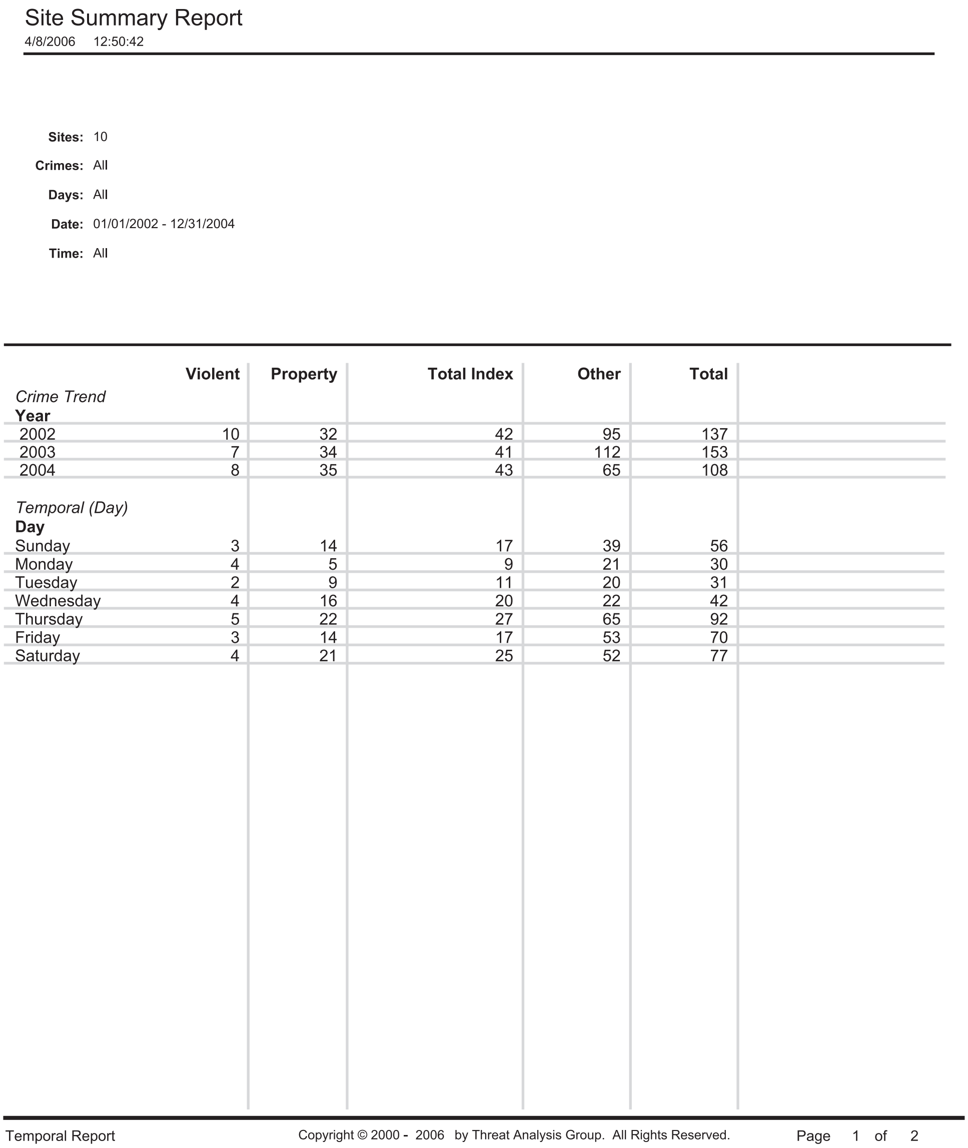


Figure 4-8.
Crime Rate Graph.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

The temporal factors of crime may be analyzed in many ways, including time of day, day of week, quarter, and seasonal trend. When a temporal pattern exists, we can deploy resources during the peak times to block the opportunities for crimes. Temporal analysis can significantly cut down the cost of a security force.

Spatial Analysis

Crime analysis focuses on *wheredunit* rather than *whodunit*—that is, where the crime occurred rather than an offender-specific crime analysis. Spatial analysis is another critical kind of analysis that helps deploy security resources efficiently by assessing the location of crime within the facility. For larger properties, spatial analysis can be very useful, but even for smaller facilities, an understanding of whether crimes are occurring inside the facility or outside in common areas such as parking lots can be beneficial in selecting countermeasures. Hot spot analysis is a form of spatial analysis in which hot spots are small places in which crime occurs so frequently that it is highly predictable. Hot spots are identified using clustering—that is, repeat events or crimes at the same place.



Site Summary Report
4/8/2006 12:50:42

Sites: 10
Crimes: All
Days: All
Date: 01/01/2002 - 12/31/2004
Time: All

	Violent	Property	Total Index	Other	Total
Crime Trend **Year**					
2002	10	32	42	95	137
2003	7	34	41	112	153
2004	8	35	43	65	108
Temporal (Day) **Day**					
Sunday	3	14	17	39	56
Monday	4	5	9	21	30
Tuesday	2	9	11	20	31
Wednesday	4	16	20	22	42
Thursday	5	22	27	65	92
Friday	3	14	17	53	70
Saturday	4	21	25	52	77

Temporal Report Copyright © 2000 - 2006 by Threat Analysis Group. All Rights Reserved. Page 1 of 2

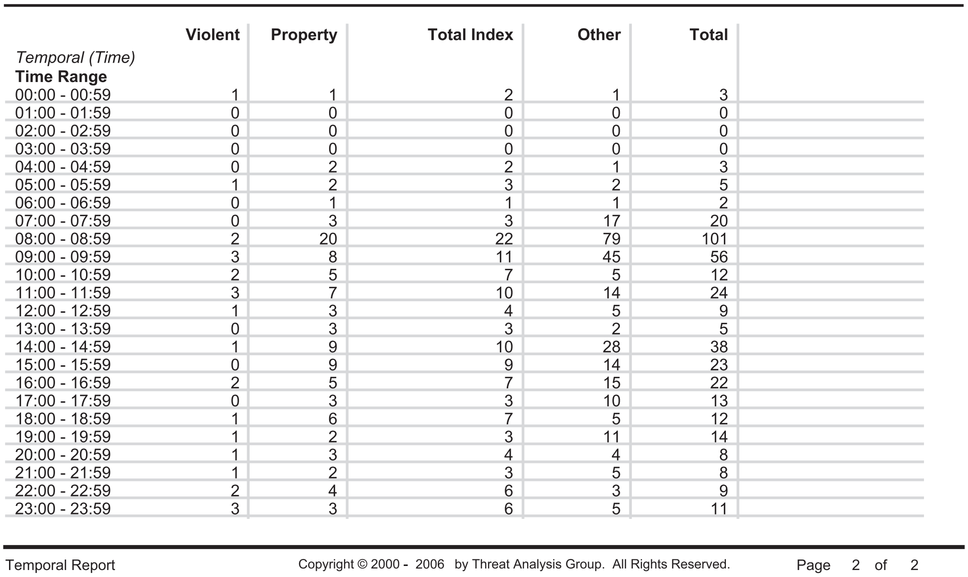
Figure 4-9.
Site Summary Temporal Analysis.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

Specifically where does the problem stem from?

Through what door did an intruder enter the property?

At what point did an attack take place between the building exit and the parking garage?

Around what certain corner was an attacker hiding before perpetrating the crime?



	Violent	Property	Total Index	Other	Total
Temporal (Time)					
Time Range					
00:00 - 00:59	1	1	2	1	3
01:00 - 01:59	0	0	0	0	0
02:00 - 02:59	0	0	0	0	0
03:00 - 03:59	0	0	0	0	0
04:00 - 04:59	0	2	2	1	3
05:00 - 05:59	1	2	3	2	5
06:00 - 06:59	0	1	1	1	2
07:00 - 07:59	0	3	3	17	20
08:00 - 08:59	2	20	22	79	101
09:00 - 09:59	3	8	11	45	56
10:00 - 10:59	2	5	7	5	12
11:00 - 11:59	3	7	10	14	24
12:00 - 12:59	1	3	4	5	9
13:00 - 13:59	0	3	3	2	5
14:00 - 14:59	1	9	10	28	38
15:00 - 15:59	0	9	9	14	23
16:00 - 16:59	2	5	7	15	22
17:00 - 17:59	0	3	3	10	13
18:00 - 18:59	1	6	7	5	12
19:00 - 19:59	1	2	3	11	14
20:00 - 20:59	1	3	4	4	8
21:00 - 21:59	1	2	3	5	8
22:00 - 22:59	2	4	6	3	9
23:00 - 23:59	3	3	6	5	11

Temporal Report Copyright © 2000 - 2006 by Threat Analysis Group. All Rights Reserved. Page 2 of 2

Figure 4-9.
Continued

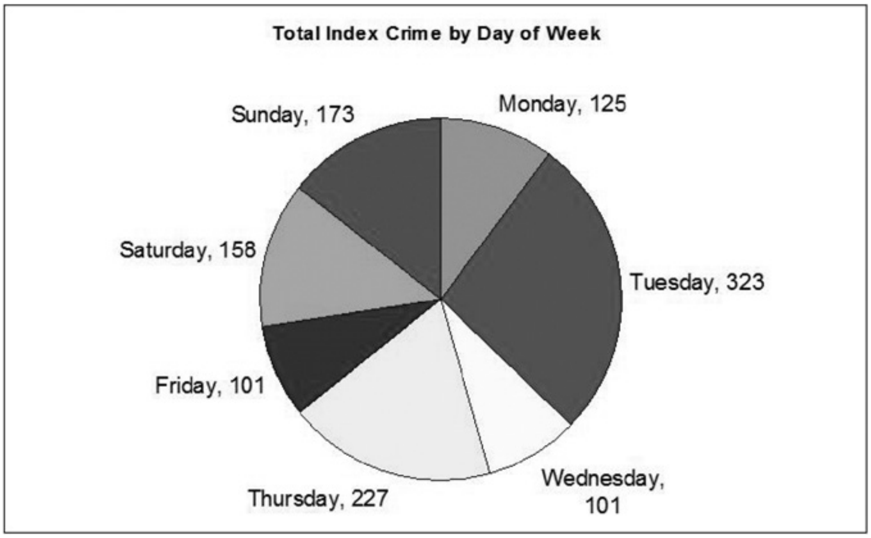


Figure 4-10.
Temporal Analysis by Day of Week.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

Knowing the answers to these questions can help determine the nature of defenses that are at the security team's disposal. For example, if the security decision maker of an office building realizes that the parking garage is the paramount source of crime, emphasizing security for the suites inside the building would certainly do little to address the problem at hand.

Spatial analysis focuses on specific targets within the property and the security measures that were penetrated. For example, if a crime pattern has been established at a particular location within the facility, the security decision maker can review the security measures currently in place as well as the access points to that area and mark them for improvement by way of personnel, physical measures, or simple policy and procedure changes.

Spatial analysis is aided by facility blueprints and other schematics of the site to help pinpoint crime scenes. If the security decision maker finds that a number of crimes are clustering in the same location, he can then look to see what opportunity there is for crime to occur there and he can attempt to block the incidents in the future.

Modus Operandi Analysis

Modus operandi, a term commonly heard in television crime dramas, 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. Dependent on the availability of details culled from in-house security reports, offense reports, or interviews with victims, witnesses, and offenders, MO analysis determines an offender's criminal tactics that separate their crimes from those of other criminals.

From modus operandi analysis, certain crime features become known. Some crimes such as purse snatchings on days when people are to be paid from their jobs might make sense when one considers what has been learned about rational choice theory and routine activity theory, 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.

Forecasting

Forecasting is a useful crime analysis technique that allows the security decision maker to mathematically project future crime by using the facility's crime history. Forecasting can project specific crime concerns as well as the times, days, and locations of these future crimes. For forecasting to be accurate, larger samples of data are beneficial, typically at least three years of data. The larger the database, the more accurate the forecasts are.

Table 4-2
Forecast.

Site ID	Crime Type	Min (68% confidence level)	Max (68% confidence level)	Min (95% confidence level)	Max (95% confidence level)
10	01—Murder	0	0	0	1
10	02—Rape	1	1	0	2
10	03—Robbery	5	7	4	8
10	04—Aggravated Assault	1	1	1	1
10	05—Burglary	0	0	0	0
10	06—Theft	14	20	11	23
10	07—Auto Theft	15	21	12	24
10	08—Arson	0	0	0	0

Once the various statistical analyses are complete, the security decision maker finds him- or herself well equipped to make decisions about future allocations of security resources. The crime analysis results should be disseminated among as many departments in the company as feasible to obtain feedback and possible solutions. Most importantly, the information should be distributed to line security officers and supervisors so that they are aware of the threats and can work toward reducing the opportunity of these crimes. Obviously, the information should be as specific as possible to enhance the detection and protection function with which the security force is charged.

Return on Security Investment (ROSI)

In today's corporate environment, it is important for all departments to show bang for the buck. This philosophy applies to the security organization all too much, for often its budget is among the first to be cut. Showing a return on investment simply means that security measures are either paying for themselves or, better, adding to the bottom line. Return on Security Investment is important because it helps the security decision maker justify costs and obtain future budget monies. Some security programs will not pay for themselves, whereas others actually become a profit center.

For example, crime analysis almost always pays for itself because it helps the security decision maker select the most appropriate security solutions for specific problems and efficiently deploy the resources. Without it, the effective security decision maker has little to guide him toward effective, adequate, and reasonable solutions. It is more difficult for more expensive countermeasures such as CCTV systems and personnel to show return on investment. Over the long run, however, these measures become relatively inexpensive when compared to the financial turmoil that can occur from even just one indefensible claim of negligent security.

A recent case study published by the American Society for Industrial Security International in Volume 6 of its *Security Business Practices Reference* discussed a retail company that was able to generate a 7 percent savings on its projected security budget using crime analysis. In order to select and deploy appropriate security measures, the retailer outsourced its crime analysis needs to the author's security consulting firm. Using the crime data generated for each of its stores, the retailer expanded its risk model from internal security reports only to include the police crime information in assessing the threat level at each of the company's retail stores.

Since the company's retail stores cater to a diverse group of people and are normally the anchor store in strip centers, a lot of the crimes reported from each store did not actually occur at the facility. Offense reports were used to verify all violent crimes in order to ensure that only those crimes that actually occurred at the property and occurred as reported were included in the database.

The security department utilized a crime analysis software application to analyze the databases of crime data for each of its stores. The database includes the time and date of each crime and the specific nature of the crime that occurred. The software allows the department to quickly determine where the violent crimes occurred on the property and to identify the victim. With this information, the security personnel are able to determine not only whether a store is high, medium, or low risk, but also who is being targeted, customers or the store itself. With this specific information, the security department can deploy appropriate security measures to reduce the risk at each store specifically.

By the end of their first year with this new program, the security department was able to realize a sizable return on investment. Based on the company's 300 stores, an annual savings, or cost avoidance, of $9.2 million was gained in the first year after implementation. This savings reflect a number of changes to the security program, but primarily constitute the redeployment of security personnel during higher risk times. Prior to this new program, security personnel were used haphazardly with no regard for actual risk levels.

Although this example is tangible, most savings in the business of security are intangible and not as easy to assess quantitatively. One of these categories is the savings generated by reducing crime and thus the avoidance of security-related litigation. Regardless of a security measure's ability to be quantitatively assessed, security decision makers should strive to calculate a return on security investment.

This page intentionally left blank