

Chapter 1

DATA-DRIVEN SECURITY

In this chapter . . .

- Need for Data-Driven Security
- Security Metrics
- Data-Driven Assessments

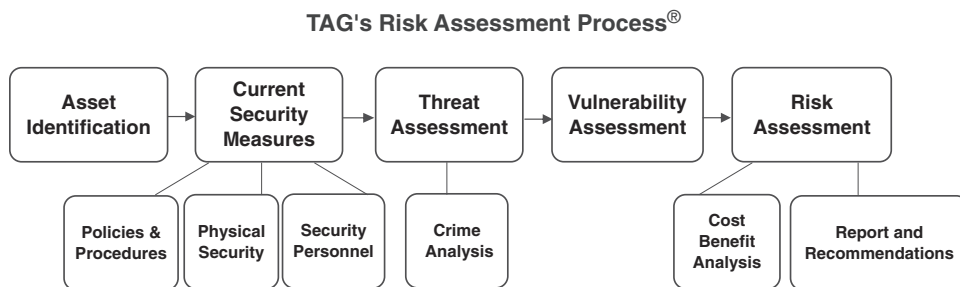


Figure 1-1.

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.

DATA-DRIVEN SECURITY

What cannot be measured cannot be managed. This is a commonly accepted business paradigm, yet its acceptance is not as far reaching within the security industry as it is in other industries. Simply put, data-driven security refers to using measurable factors to drive a security program. While not all elements

of a security program lend themselves to measurement, many components can be measured effectively. For example, physical protection systems are measured via penetration times, and barriers are measured using delay and defeat times. Other security components can be measured, though not mathematically, including morale of protection forces.

Some would argue that security is more of an art than a science. While they are correct, the business of security is not an art per se. The security department is a business unit not unlike other business units within a company that must justify their existence. The higher security moves up the corporate ladder, the more challenges the security director will face and the more business acumen will be required. Given the security industry's growth out of public law enforcement, it is no surprise that it has taken the industry this long to develop into a full-fledged corporate entity. With this growth comes the need to depart from the police mentality. Twenty years ago, most security directors were retired law enforcement agents who made the jump to private security as a way to supplement their retirement income. This has proven to slow the growth of security within the corporate hierarchy, but it was probably a necessary step in the history of the industry. This is not to say that retired law enforcement personnel do not have a place in the security industry. To the contrary, many have proven to be exemplary business security leaders who have made significant leaps for the security departments in their companies.

As the security industry grows to include not only physical security, but also information technology security, it is incumbent upon today's security directors to focus more on the business than operational side of security. This necessity is best summarized by the world's leading security association, ASIS—International, in its Chief Security Officer Guideline:

Today's business risk environments have become increasingly more severe, complex, and interdependent, both domestically and globally. The effective management of these environments is a fundamental requirement of business. Boards of Directors, shareholders, key stakeholders, and the public correctly expect organizations to identify and anticipate areas of risk and set in place a cohesive strategy across all functions to mitigate or reduce those risks. In addition, there is an expectation that management will respond in a highly effective manner to those events and incidents that threaten the assets of the organization. A proactive strategy for mitigation of the risk of loss ultimately provides a positive impact to profitability and is an organizational governance responsibility of senior management and governing boards.

The guideline goes on to discuss the role of the chief security officer (CSO) as a business leader, a problem solver, as well as an expert in security for their company. Interestingly, the guideline also suggests that the CSO's background

includes business, not law enforcement, since the CSO's key responsibility "is to develop and implement a strategy that demonstrates the processes in understanding the nature and probability of catastrophic and significant security risk events." As the company security departments grow and begin to encompass more responsibility for the protection of people, property, and information, so too must the ability to fall back on empirical data to support our position. No longer can security professionals rely solely on gut instincts.

Too often recommendations from the security department are presented with little or no thought to why certain procedures or security equipment should be used. Often, a security measure is deployed because other companies are doing it. It is all too common in the security industry for there to be a propensity for using certain security measures without complete understanding of the problem or a thorough analysis of the security measures' ability to be effective in a given situation. Data-driven security can help security directors overcome this problem by identifying key concerns, the specific security measure's ability to solve the problem, and the anticipated cost.

How can security professionals justify to senior executives a sizable and usually growing annual security budget? By now, most security directors are keenly aware that a security program's success depends on the commitment and support, or buy-in as it is commonly known today, of senior executives. Using anecdotal evidence to justify spending on physical security measures and costly protection personnel no longer suffices. A data-driven security program helps management understand that security is more than a must-have expense; it justifies costs to management by showing the proof of success that, when presented effectively, can garner the necessary buy-in from upper management and demonstrate a convincing return on investment. Security expenditures, just like other departmental budgets, need to be justified with empirical data and supplemented with cost-benefit analyses and comparisons.

Throughout the first part of this book, various assessments used in the security industry are discussed, including threat, vulnerability, and risk assessments along with specific types of assessments such as crime analysis. Common to each of these assessments is a quantitative approach to establish a baseline from which security effectiveness can be measured. Assessments are the foundation on which a security program is built by establishing a baseline of risks that companies face. They guide the strategic planning and design of countermeasures intended to mitigate those risks.

Such a logical approach brings benefits that are unattainable with qualitative assessments, which are still used throughout the public and private security sectors. While qualitative assessments cannot be abandoned, their use should be limited to those instances where quantitative ones cannot be used for lack of measurable elements. Thus, physical security is, and shall remain, more of an art than a science, though science can be infused into an otherwise abstract industry.

I don't care how skilled you are as a diplomat or how brilliant you are at leading, if you are not professional about security, you are a failure.

—U.S. Secretary of State Madeline Albright

SECURITY METRICS

Between September 2001 and the writing of this book in April 2006, the United States suffered no major terrorist attacks. Although this fact makes for a great sound bite for political talking heads, it is not an accurate metric of the true threat faced by the United States. A more appropriate metric would be the number of attacks thwarted since September 2001 or the number of arrests made of known terrorists. When providing asset protection, accurate measurement of security effectiveness can have a profound impact on management's level of support for the security department.

As we have discussed, a common paradigm in business is that an activity cannot be managed if it cannot be measured. Security is one such activity. Security metrics communicate vital information about security activities and drive decision making. Metrics for various security components, such as the protection force or access control system, can be an effective tool for security professionals to understand the effectiveness of the overall security program. Metrics, as previously mentioned, may also identify risk based on failures or successes of security components, and can provide solutions to security problems. Security metrics focus on the results of security decisions such as a reduction in thefts after implementation of a CCTV system, an increase in visibility after a change in security officer uniforms, or a reduction in terrorist acts as a result of terror cell arrests.

Security metrics help define how secure we are. They assist security professionals in answering basic questions posed by management, such as:

- Are company assets protected?
- Which assets need more protection?
- Can the asset protection program be improved?
- What resources should be allocated to security?
- How does our company compare to others?
- Are we reducing our liability exposure?

The National Institute of Standards and Technology (NIST) defines metrics as tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. Thus, security metrics assist security professionals in making asset protection decisions through the measurement of performance-based characteristics of security components. Simply stated, security metrics are tools used for measuring a company's security posture.

For the security metrics to be accurate, security professionals must have two elements in the metrics model:

1. Proper performance data for the specific countermeasure under evaluation.
2. An appropriate baseline from which to compare.

Baseline measurements are often difficult to obtain, especially in the business of security where companies are, out of necessity, secretive about their protection systems. In recent years, security industry associations such as ASIS—International, the National Fire Protection Association, and the International Association for Professional Security Consultants have promulgated standards, guidelines, and best practices. In addition to published and accepted industry standards, the courts have outlined baselines of measurement for the security industry. An example 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: recency, proximity, publicity, frequency, and similarity of past crimes. An example of crime metrics legislation is the 1996 Illinois Automated Teller Machine Act (ATM). Section 20 of the Act provides procedures for evaluating the safety of ATM regarding “the incidence of crimes of violence in the immediate neighborhood of the ATM.” Texas has a similar ATM Safety law which requires that financial institutions collect crime metrics. Thus, the professional security practitioner will stay abreast of industry standards and the law. While laws must normally be reasonably followed, security professionals may fine-tune published industry standards to meet the needs of their company.

In addition to establishing a baseline for comparing company metrics, metrics are also used to justify budgets, provide data for decision making, and improve security practices.

Metrics can be used to justify budgets and provide the basis for obtaining additional monies for the security department. Security metrics may be plugged into cost-benefit analyses to identify the need for various security components. For security decision making, metrics can unveil trends and patterns in the security program’s performance from which security decision makers can make decisions to modify the program. For example, once a physical protection system is alerted of an intruder, security force personnel normally respond. By measuring the time needed to respond from the security officer’s fixed post to the breached access point, the security decision maker can determine if the response time is adequate or if another post needs to be established closer to the access point. Finally, metrics assist in the development of good security practices. An example may be found in the use of security personnel to provide escorts for company personnel exiting the building to the parking areas. Although this is a common practice in some companies, an analysis of security

incidents during peak times may indicate a sharp increase in security breaches because security personnel are distracted from their primary protection duties while escorting personnel. In this instance, the value of providing escorts must also be considered in determining the company's security practices.

SMART METRICS

Good metrics are attainable when security professionals strive for metrics that are SMART—Specific, Measurable, Actionable, Relevant, and Timely.

Specific—a metric must measure a specific variable.

Measurable—a metric measures what is measurable. Not all components of a security program are measurable. For example, morale among security forces is often “measured” but not in a quantitative manner.

Actionable—a metric should not measure variables that cannot be acted upon. If a security decision maker cannot remedy a problem, there is not much sense in wasting time on that variable.

Relevant—a metric that fails to provide any information to improve the security program should be avoided. If the metric cannot tell us where we can improve, it is not relevant.

Timely—metrics have expiration dates. Historical data are an excellent indicator of the future; however, the older the data, the less important they may be. A metric system incapable of assessing the latest data is useless.

As discussed in the introduction to security metrics, the number of attacks against the country or the number of crimes at a location may not be the best indicator of an effective security program. While luck does play a part in the protection game, there are other factors that can be measured in answering the question of how secure we are. To develop a security metrics system, security professionals can adapt the Six Sigma methodology used to eliminate defects. The author has successfully implemented a variation of this methodology for use with protective forces within the federal government. The methodology involves seven steps that may be easily modified for our use in security metrics:

1. Define the metrics system goals.
2. Decide what metrics to generate.
3. Develop strategies for generating the metrics.
4. Establish benchmarks.
5. Develop a metrics reporting system.
6. Develop and implement an action plan.
7. Create a formal system review cycle.

Going through each step in detail should enable security professionals to adapt the methodology to their needs.

The only security is the constant practice of critical thinking.

—William Graham Sumner

Step 1: Define the metrics system goals.

Critical in today's business environment is the need to set performance-based goals. Setting high, yet reasonable, goals during the development of a security metrics system is a necessary step. The goals should be well-defined and based on the needs of the security department, though continued refinement of the goals while moving through the seven steps is acceptable. Each goal should clearly state the desired result to which all metrics collection and analysis efforts are directed. An example of a metric goal within the personnel department of a security program is, "The response time metric shall clearly communicate to supervisors the average time needed for a security officer to patrol and secure the fifth floor office space."

Step 2: Decide what metrics to generate.

Deciding what to measure is crucial to an effective metrics system. As referenced earlier in this chapter, during the five-year period covered since the September 11, 2001 attack and the writing of this book, the United States has suffered no major terrorist attacks. This is obviously good news, but it is not a true measure of our vulnerability. Thus, Step 2 is to identify the specific security components or practices that have kept us free from terrorism. One example of this is the number of arrests of known terrorists within U.S. borders. Another example may be the number of attacks thwarted due to intelligence efforts.

Step 3: Develop strategies for generating the metrics.

Collecting the data for metrics can be a daunting task. The security professional's strategy for data collection should identify the source of information and the frequency with which that raw data is collected by the source. It is not uncommon for a security decision maker to require data from other departments. Successful identification of the sources is key to a sound metrics program. An example can be found in crime analysis. Security decision makers often use traffic levels at a facility to calculate the crime rate at that facility. While the security department itself typically does not have any way to determine how many people pass through a facility in a given day, month, or year, other departments normally do have this data. The security professional must therefore seek out that source and ensure that the data meets the quality control requirements of the metrics system.

Step 4: Establish benchmarks.

As we have noted, there are both industry benchmarks and internal benchmarks from which to compare. Benchmarking may be defined as the process

of identifying and adapting outstanding security practices from organizations within the industry for the purpose of improving company security practices. In the crime analysis field, the author has had the opportunity to evaluate both internal and external crime reporting systems at many companies. With this information, the author has been able to improve the reporting systems for one client based on the system at another company.

Step 5: Develop a metrics reporting system.

The collection and analysis of metrics is not enough to improve the security program. The system must also include a reporting component whereby those who carry out the line function can work to improve their work. Effective communication is vital to the metrics system. The frequency, content, and method of dissemination of reports should also be established at this step. Continuing the example used in Step 1, collecting and analyzing response times does not in itself correct the problem. The security department must communicate the results to line personnel supervisors so that corrective action can be taken.

Step 6: Develop and implement an action plan.

A security metrics action plan guides the users toward the end result. The plan identifies and defines all tasks required for the metrics system to be effective, as well as a time line of events leading up to reporting of metric results. The plan should be written and available to everyone involved in the program.

Step 7: Create a formal system review cycle.

Similar to the business environment, security is dynamic and must be adjusted to the needs of the day. A formal system review at regular intervals ensures that the security department is measuring what it should be measuring. With time, things change and more security components may be added to a security program which require metrics generation, while other components are removed and no longer require metrics.

Developing a security metrics system is time consuming, but can prove to be a panacea for a security department. The methodology outlined here makes the process easier and should be adapted to meet the security department's needs. The incentive for this project is that the resulting security program will not only be effective within the company, but may also be regarded as the benchmark by other organizations.

DATA-DRIVEN ASSESSMENTS

This section briefly introduces the reader to the various definitions and tools used throughout the remainder of this book. Each topic presented in the following paragraphs will be discussed in depth in later chapters. Among the more commonly used terms are *threats*, *vulnerabilities*, and *risks*. Although various definitions are used in the industry and many people use these terms interchangeably, this book will attempt to clarify the differences among definitions.

Generally speaking, threats are things that can go wrong or that attack the system. Examples include natural disasters and people. Vulnerabilities are those things that make the facility more prone to attack by the threats. Vulnerabilities are exploited by threats. For example, a lack of access control may be a vulnerability that can be exploited by a person. Risk is a function of threats and vulnerabilities. Countermeasures are things that reduce or block opportunity for threats to exploit vulnerabilities. They are preventive in nature. An access control system is a countermeasure that can block entrance by a threat.

Whether security assessments are vulnerability, threat, or risk assessments, the primary goal should be to make the process as objective as possible. The two types of assessments are quantitative and qualitative; both can and should be utilized depending on the scenario.

Qualitative assessments, on one hand, are normally used when the assets in need of protection are of lower value or when data is not available. The results of qualitative assessments depend on the assessment skills of the people involved in the assessment. Risk levels are normally given in abstract values such as high, medium, or low, or they are color coded as in the Homeland Security Advisory System.

Quantitative assessments, on the other hand, are metric based and assign numeric values to the risk level. Overall risk levels are derived from all available security metrics. In a physical protection system, for example, the metrics used in determining the risk level include the threat level, probability of detection, delay times, and response force times. Quantitative assessments are commonly used for the protection of business critical or high-value assets.

Threat assessments, as discussed earlier, identify things that can go wrong or that attack the system. When focused on the people threat, threat assessments ask who the bad guys are. Today, more than ever, racial profiling has come to the forefront of the public's attention. Since the September 11 attacks, Arabs have come under greater scrutiny much as was the case with the Japanese during World War II. Without getting into the politics of this issue, it is safe to say that racial profiling is a form of threat assessment. Crime analysis, as discussed in depth in the following chapter, is a type of threat assessment that focuses on third-party crimes.

Vulnerability assessments identify weaknesses in a security program without regard to the threats. Vulnerability assessments are common in business continuity planning where loss of assets is considered. The U.S. military has a number of declassified documents that outline vulnerability assessments. One such document is the United States Army Training and Doctrine Command Regulation 525-13 for Force Protection Programs (FPP). Vulnerability assessments may also be quantitative or qualitative, though quantitative assessments are fairly easy to accomplish since the emphasis is on assets whose values are typically known.

Finally, risk assessments are comprehensive and logical reviews that look at both threats and vulnerabilities. They can be both quantitative and qualitative,

or they can be a hybrid. This type of assessment thoroughly evaluates the overall risk, including asset identification, threat analysis, and vulnerabilities in the day-to-day operations of the facility or the company. Assets include people, property, and information. Qualitative assessments are based on the data available and the skills of the assessment team, whereas quantitative assessments utilize numeric data to evaluate risk. Risk assessments are typically a staged process whereby critical assets are identified, current countermeasures are enumerated, threat and vulnerabilities are defined, and prioritized recommendations are made to protect critical assets based on probabilities of attack. The first two steps of the risk assessment methodology, asset identification and security inventory, are discussed in Chapter 2.

General Characteristics of a Comprehensive Risk Assessment Methodology

- Designed for a specific organization or industry
- Complies with regulations and is guided by industry best practices
- Designed for information technology security, physical security, or a combination of both
- Categorizes assets based on criticality to the organization's mission
- Identifies existing security measures used to protect assets
- Determines threats using multiple sources
- Uses tools and techniques to identify vulnerabilities
- Analyzes risk to assets based on threats and vulnerabilities
- Recommends multiple strategies for reducing risk