USING THE CRITICAL ASSET AND INFRASTRUCTURE RISK ANALYSIS (CAIRA) METHODOLOGY

The All-Hazards Approach to Conducting Security Vulnerability Assessment and Risk Analysis

By Doug Haines

In order to accomplish its primary function or reason for being, every organization must protect personnel and critical assets from all hazards, both natural and man-made.

Spending limited funds to protect personnel and not spending funds on the buildings they occupy or the infrastructure that supports those buildings and vice versa is unacceptable. Not only must organizational leaders make every effort to ensure that organizational resources are adequately protected but they also must ensure that in the unlikely event a catastrophic scenario occurs, they reduce injury to personnel and mass casualties and the continuity of operations. This can be an extremely delicate balancing act in risk management for those in leadership positions.

Without a quantitative method for risk assessment and analysis, this question cannot be truthfully answered. By responding, "I think I'm protecting everyone and everything", simply won't cut it.

Risk Management

The first thing to understand about risk management is that it does not mean risk avoidance. You must first accept the fact that not all risks can be avoided and some level of risk remains no matter how many countermeasures are in place. Smart and confident organizational leaders will understand this principle and accept it. Now some folks will argue that if enough countermeasures are put in place then total risk can be avoided. This is simply not true. While you may be able to reduce to a level that a successful manmade threat is highly improbable, you will never be able to eliminate the threat or all hazards completely. Natural events occur on a frequency all their own. Some events occur every year; i.e., snowstorms, hurricanes, tornadoes while others occur every thousand years, flooding, earthquakes, volcanic eruptions. So the question is, "Why is it that, even after I've spent all this money and I dealt with every conceivable hazard scenario, the event still occurred". Well, think of it this way, you get routine maintenance done on your car; you change the oil, rotate the tire, etc. , yet sometimes things just break and the car sits on the side of the road waiting for the repair truck. By getting your car serviced regularly you are lowering your risk from the hazards of over-heating, uneven tire wear, parts breaking and so on. In essence, you lowered the risk

but you didn't avoid it. The same holds true for security. Some hazards may be mitigated to the point where it is very improbable that they will occur and others may not be completely prevented no matter how much you spend. The risk can be reduced to a level that is acceptable but not completely avoided (See *Figure 1*).

The keys principles in risk management are:

1) lowering the likelihood that the event will occur and accepting some level of risk, and
2) minimizing its affects in the unlikely event it happens

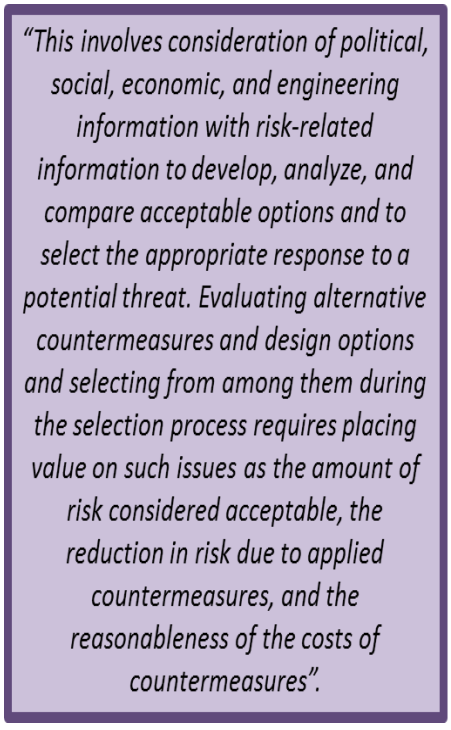


Figure 1. **Risk Management as Defined in Security Engineering**

Qualitative versus Quantitative Analysis

The best way to calculate risk is by conducting a risk assessment. There are two types of assessments – Qualitative and Quantitative.

Qualitative Analysis

The qualitative methodology relies on the individual's expertise in the subject matter to provide for a valid assessment.

This reliance is one of four disadvantages in using this type of methodology. Lacking consistency over time is another disadvantage, as the assessor is likely to rate criticality at a lesser level based on familiarity or complacency. Another disadvantage is that there is no standardization of values. One person may give a high value while another assessor may provide a lower score for the same item. One way to compensate for this factor is to have a team of people to do the assessment and take an average rating of the group. As you know, however, getting a group of people together and having them agree on anything is easier said than done. The fourth disadvantage is that outside influences can affect the outcome or the assessor can be unduly persuaded to rate items at a certain value in order to achieve a desired result.

That said, one advantage to the qualitative methodology is that just about anyone can do it, with little or no experience, based on their "gut feeling". They only have to hope that they get it right.

Quantitative Analysis

Quantitative assessment resolves the disadvantages of lack of consistency overtime, lack of subject matter expertise, lack of standardization and outside stimuli common in qualitative analysis.

Each item that is evaluated is given a number value; therefore, it provides standardization. Since those values don't change regardless of who's doing the assessing, it fixes the other three problems of qualitative analysis. It provides consistency over time and is not dependent on a person's level of experience nor can it be manipulated to achieve a specific result.

Because of this standardization, quantitative mirrors qualitative – in that – anyone can do it. They just point and click, if you will.

A quantitative risk analysis and vulnerability assessment methodology called CAIRA (Critical Asset and Infrastructure Risk Analysis, pronounced Sear-Ra) has been developed by Haines Security Solutions (HSS) in identifying and measuring risks and determining the most cost-effective countermeasures for mitigating those risks.

HSS is recognized as a center of expertise within the security community for risk assessment, providing services for many Federal, State, local government agencies and private companies around the globe.

A typical assessment team is made up of subject matter experts specializing in physical and technical security, law enforcement, forced-entry tactics, electronic security systems, antiterrorism, force protection, engineering, criminal and terrorist intelligence, logistics, and quantitative analysis.

The CAIRA Approach

A holistic approach is taken to analyzing natural and manmade hazards. The process looks at the most common naturally occurring hazards; such as, heavy rain/flooding, tornados, earthquakes, etc. It also takes into consideration an asset's location. For example, is the asset and its supporting energy infrastructure (electric, fossil fuels, steam or water) located in an area prone to volcanic eruption or heavy snow storms? It calculates risk based on probability of occurrence. Generally speaking, the higher the likelihood of the event the higher the risk is to the asset from that particular type of hazard. CAIRA also analyzes manmade hazards; ranging from a disgruntled employee bringing a gun to work to acts of vandalism to a bombing due to a terrorist act.

CAIRA is a quantitative assessment that differs from a qualitative assessment because it uses fixed numerical values to evaluate the hazards, target criticality, vulnerabilities and risks.

The results of the analysis can be used as the basis for making informed decisions by organizational leaders.

Because risk is quantifiable, it becomes a yardstick that can be used to make decisions about allocating resources – facilities, funding, property and personnel.

In CAIRA, security countermeasures are selected based on their likelihood of lowering the risk to the asset, as well as, their cost effectiveness. In many cases, risk analysis and risk management become an optimization analysis that examines risk reduction values (due to implementing countermeasures) and the associated costs to implement the identified remedies through a simple cost–benefit study.

Although performing a detailed risk assessment is complicated, following the CAIRA methodology makes it manageable.

The results are tailored to an organization's needs and can be used to

make informed decisions in the allocation of resources to mitigate risks.

CAIRA Methodology

The primary purpose of CAIRA is to quantitatively measure hazards or threats, asset criticality, vulnerabilities, and risks to energy systems associated with large compounds or small government or private facilities. It establishes a security baseline, explores upgrades, recalculates vulnerabilities and risks, and recommends optimized features or improvements for facilities. In essence, CAIRA identifies current levels of vulnerability and risk and then identifies improved levels with the implementation of specified countermeasures – basically a snapshot of where the organization is today and where it could be after countermeasures are implemented.

In addition, CAIRA identifies the associated cost and impact of the improvements. CAIRA includes the performance of six sub-analyses: hazards, target, vulnerability, optimization, risk, and cost–benefit.

Hazards Assessment (Likelihood and Severity)

In all, 38 natural hazards and 22 manmade hazards are analyzed during the Hazards Assessment. This information produces a hazard rating (See *Figure 2*), which measures the likelihood or probability of the hazard occurring and an effectiveness rating, which indicates the severity of the occurrence and its impact on operations in both manpower and financial terms.

The likelihood of occurrence, the resulting severity and asset resiliency are calculated and stated as a percentage.

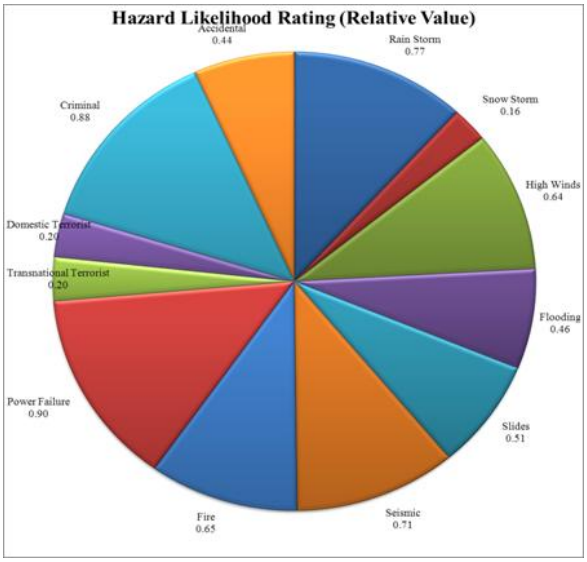


Figure 2. **Hazard Likelihood Rating (Relative Value) Pie Chart**

Target Analysis (Criticality Assessment)

Target analysis is designed to evaluate and measure the value of all targets to the user and in the case of manmade threats, to the aggressor. Targets could include any type of asset or target including facilities, people, equipment, money, processes and systems. The end result of the target analysis is a numeric rating based on the target value or criticality to the user and the target value or usefulness to the aggressor.

Baseline Vulnerability Analysis

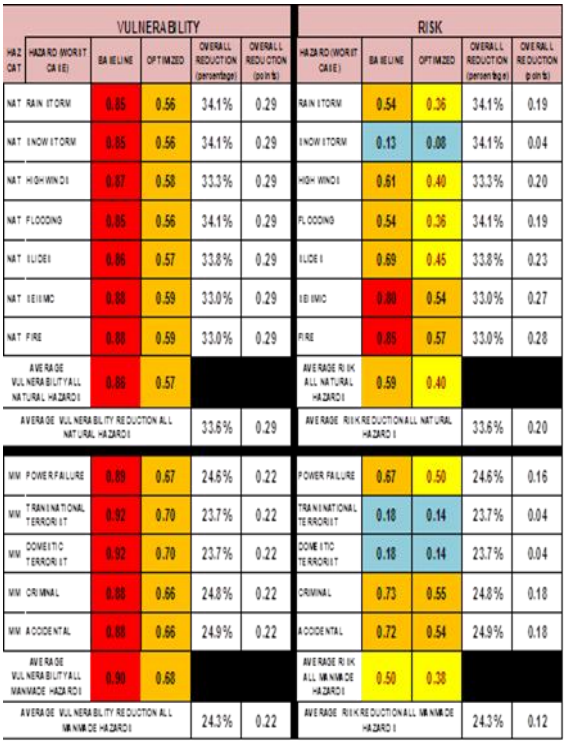
Vulnerability analysis is designed to quantitatively evaluate and measure how vulnerable a specific asset is to a specific hazard. This phase of CAIRA identifies the countermeasures currently in place for a specific target is assigned a value based on their effectiveness in mitigating hazards (Baseline Vulnerability Rating [BVR]).

Optimized Vulnerability Analysis

Optimization analysis is the reapplication of the vulnerability analysis after implementing hypothetical improvements resulting from countermeasures that could be used for a specific asset. Hypothetical countermeasures could include programmatic or procedural options. The end result is an optimized vulnerability rating (OVR) associated with the specific target being analyzed. Based on the optimization analysis, the average vulnerability and risk rating can be identified and stated as a percentage.

Risk Analysis

Risk analysis (See *Figure 3)* is the aggregation of the hazards, target, vulnerability, and optimization analyses to determine the calculated value of risk associated with a specific asset that is being influenced by a specific hazard.



VULNERABILITY					RISK				
HAZ CAT	HAZARD (WORST CASE)	BASELINE	OPTIMIZED	OVERALL REDUCTION (percentage)	OVERALL REDUCTION (points)	HAZARD (WORST CASE)	BASELINE	OPTIMIZED	OVERALL REDUCTION (percentage)	OVERALL REDUCTION (points)
NAT	RAIN STORM	0.85	0.56	34.1%	0.29	RAIN STORM	0.54	0.36	34.1%	0.19
NAT	SNOW STORM	0.85	0.56	34.1%	0.29	SNOW STORM	0.13	0.08	34.1%	0.04
NAT	HIGH WIND	0.87	0.58	33.3%	0.29	HIGH WIND	0.61	0.40	33.3%	0.20
NAT	FLOODING	0.85	0.56	34.1%	0.29	FLOODING	0.54	0.36	34.1%	0.19
NAT	FLUDE	0.86	0.57	33.8%	0.29	FLUDE	0.69	0.45	33.8%	0.23
NAT	SEISMIC	0.88	0.59	33.0%	0.29	SEISMIC	0.80	0.54	33.0%	0.27
NAT	FIRE	0.88	0.59	33.0%	0.29	FIRE	0.85	0.57	33.0%	0.28
AVERAGE VULNERABILITY ALL NATURAL HAZARDS		0.86	0.57			AVERAGE RISK ALL NATURAL HAZARDS	0.59	0.40		
AVERAGE VULNERABILITY REDUCTION ALL NATURAL HAZARDS				33.6%	0.29	AVERAGE RISK REDUCTION ALL NATURAL HAZARDS			33.6%	0.20
MM	POWER FAILURE	0.89	0.67	24.6%	0.22	POWER FAILURE	0.67	0.50	24.6%	0.16
MM	TRANSNATIONAL TERRORIST	0.92	0.70	23.7%	0.22	TRANSNATIONAL TERRORIST	0.18	0.14	23.7%	0.04
MM	DOMESTIC TERRORIST	0.92	0.70	23.7%	0.22	DOMESTIC TERRORIST	0.18	0.14	23.7%	0.04
MM	CRIMINAL	0.88	0.66	24.8%	0.22	CRIMINAL	0.73	0.55	24.8%	0.18
MM	ACCIDENTAL	0.88	0.66	24.9%	0.22	ACCIDENTAL	0.72	0.54	24.9%	0.18
AVERAGE VULNERABILITY ALL MANMADE HAZARDS		0.90	0.68			AVERAGE RISK ALL MANMADE HAZARDS	0.50	0.38		
AVERAGE VULNERABILITY REDUCTION ALL MANMADE HAZARDS				24.3%	0.22	AVERAGE RISK REDUCTION ALL MANMADE HAZARDS			24.3%	0.12

Figure 3. **Typical CAIRA Vulnerability and Risk Reduction Chart**

Cost–Benefit Analysis

Cost–benefit analysis compares the potential results of specific countermeasures for reducing or mitigating hazards against specific assets. The cost–benefit analysis is based on cost versus reduction in vulnerability and risk.

A Quantitative Measurement

CAIRA is a quantitative assessment using mathematical equations to calculate and measure asset value, hazards likelihood, vulnerability and risk versus the standard vulnerability assessment process, which is a qualitative or subjective assessment that normally focuses on compliance to regulatory requirements.

Both methodologies identify vulnerabilities and recommend countermeasures to mitigate those vulnerabilities; however, CAIRA goes further because it identifies current values of vulnerability and then reassesses those values of vulnerability based on implementation of recommended countermeasures.

Not only does CAIRA provide quantitative measurements of vulnerability and risk, it also provides cost estimates for the recommended countermeasures developed as part of the assessment process if they were to be implemented. Knowing the BVR and comparing it to the OVR and then calculating the cost to reach the OVR, the CAIRA methodology produces a cost–benefit analysis that can be used to prioritize countermeasures or compare one facility to another.

In Summary

To summarize, CAIRA quantifiably measures vulnerability and risk, prioritizes recommended countermeasures, prioritizes facilities, and compares cost and countermeasure effectiveness. Most importantly, CAIRA lets the customer know how vulnerable the asset is, what to do to reduce the vulnerability, how effective the recommendations will be in reducing the vulnerability, and at what cost.

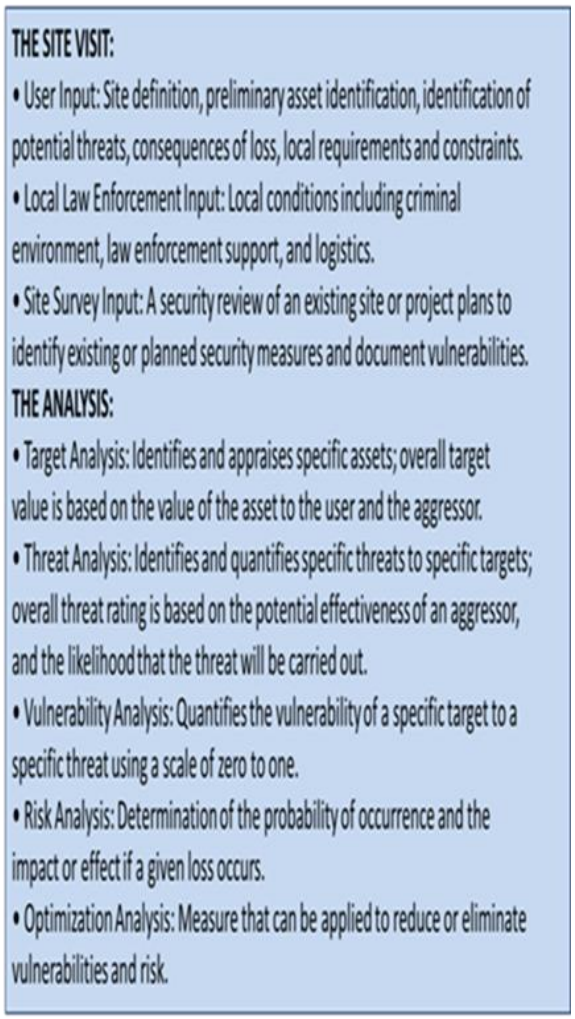


***Figure 4*. Major Elements of the CAIRA Process**

Regardless of the type of analysis or study, the resulting recommendations need to be based on a given hazards. As it relates to designing physical measures to counter the identified hazards, the HSS team performing CAIRA must have a clear understanding of the design basis hazards (DBT) to make appropriate and cost-effective recommendations.

The performance of CAIRA is not driven by regulation or design standards; therefore, the Design Basis Threats (DBT) must be identified before recommendations can be generated. HSS works with the customer to identify Single-Point Failures and other critical assets or processes within the organization.

Unlike standard vulnerability assessments, CAIRA quantifies risks and vulnerabilities, determines the cost effectiveness of specific improvements, and helps prioritize countermeasures. This in turn allows decision makers to plan for and seek hard-to-get funding.

Further they can go to bed at night knowing that countermeasures they have implemented effectively reduce the risks to personnel and facilities. Both of which translate directly to organizational productivity and cost savings.