



Identifying Vulnerability

Enhancing Organizational Security in the Post 9-11 World

Michael Taylor

President and Chief Executive Officer

American International Security Corporation



American International Security
CORPORATION

Corporate Headquarters

One Boston Place
Boston, MA 02108
1-800-852-2714

info@aisc-corp.com
www.aisc-corp.com

Identifying Vulnerability

Enhancing Organizational Security in the Post 9-11 World

Executive Summary

The devastating terrorist attacks of September 11 have fundamentally altered how American corporations and organizations view risk. Security management and its relationship to business continuity planning are no longer an afterthought on corporate agendas. The threat of terrorism has now been added to the list of potential security risks that companies must consider and for which they must develop countermeasures.

Faced with this awareness of previously unforeseen vulnerabilities, organizations are reevaluating their fiduciary and security obligations to customers, shareholders and employees. A critical component of this reevaluation is a properly implemented Vulnerability Assessment. A meaningful assessment reviews businesses vulnerabilities from both a strategic and tactical perspective, identifying risks to people, property, equipment and systems of distribution. Once the assessment has been completed, management is presented with recommendations on the reduction or elimination of key vulnerabilities.

This paper will address the proper methodology an organization should utilize to effectively define the relationship between its assets (intellectual property, customers, shareholders, employees, distribution systems and facilities), and the consequence of loss, damage or interruption of service. It is only when this relationship is quantified with an effective Vulnerability Assessment that proper security measures can be put in place.

This paper will also introduce innovative counter-terrorism techniques that American International Security Corp. (AISC) is utilizing to transform the practice of conventional risk assessment in light of the new security environment corporations and organizations now face.

The components of Vulnerability Assessment

A Vulnerability Assessment is an examination of the interrelationships between assets, threats, vulnerabilities and countermeasures. This process identifies the probable risks impacting an organization and provides the information required to implement cost-effective security practices and procedures.

Because assets have differing values, an examination is required to determine the investment required to properly secure them. Some assets are indispensable to the continuation of the business and must be protected even if it requires a significant corporate expenditure. The assets of greatest importance to an organization are the vulnerabilities associated with its people. Customers, vendors, employees and the public may all be at risk should a corporation fail to secure itself properly. The untold human cost, the legal and public relations implications and the financial consequences of weak or ineffective security can destroy an organization. Other assets may have a specific economic value and the organization needs to understand the relationship between the value of the asset and the cost to secure it.

The Vulnerability Assessment process starts when risks are identified and prioritized and follows through until effective countermeasures are implemented, tested, and evaluated. After this process is completed and a security framework established, an evaluation and testing phase will ensure that any new vulnerabilities that emerge will be identified, leading the organization back to the start of the risk analysis process.

There are four primary steps involved in a Vulnerability Assessment including:

- **Asset Analysis:** critical assets (people and property) requiring protection are identified and prioritized.
- **Threat Analysis:** potential threats are identified and assessed based on current events, industry, intelligence and historical data.
- **Vulnerability Analysis:** potential vulnerabilities are quantified on the basis of Asset and Threat Analysis and the effectiveness of existing security countermeasures are tested for effectiveness.
- **Security Policy Definition:** is formulated when countermeasures needed to reduce vulnerabilities are identified and then evaluated on the basis of cost/benefit analysis.

In the **Asset Analysis phase**, the assessment team (comprised of counter-terrorism experts with military and law enforcement experience) identifies assets and determines the impact to the enterprise if the assets were damaged or destroyed. Using this information the assets are prioritized based on the potential consequences of their loss. Also included in the asset analysis is the identification of unwanted events that could adversely affect the value of these assets.

In the **Threat Analysis phase** the assessment team determines which adversaries or events are most likely to cause harm to the assets. To determine the threat level, the team will review and access information related to current events, industry attractiveness as a target, historical information and intelligence about the capabilities and intent of potential terrorists or criminals.

Completion of the **Asset and Threat Analysis** provides the data for an effective **Vulnerability Analysis**. This phase requires the assessment team to analyze an asset through the eyes and mind of a terrorist or criminal. The team must answer questions such as:

- If I were a terrorist or criminal (or disgruntled employee), how would I attempt to destroy this asset?
- What is the probable impact if the asset is damaged or lost to a terrorist, criminal or disgruntled employee?
- How likely is it that a terrorist, criminal or disgruntled employee will attack the identified assets?
- What are the most likely vulnerabilities that the terrorist, criminal or disgruntled employee will target?

During the Vulnerability Analysis phase, a matrix is developed to show the relationship between asset, threat and consequence of loss. The matrix shows which assets face the highest probability of attack and which threats pose the greatest risk to the organization so that vulnerabilities can be rated as to their overall risk to business continuity.

When the relationship among assets, threats and vulnerabilities is thoroughly understood, then the formulation of **Security Policy Definition** or countermeasures begins. If these Security Policies are to remain effective, the organization must be committed to a continuing process of testing and re-evaluation. When countermeasures are not periodically tested, then the existing Security Policies cannot be trusted to work as planned.

Identifying Vulnerability Post 9-11 with the C.A.R.V.E.R. Matrix

Given the altered security environment in the U.S. and our asset bases around the world, organizations require a Vulnerability Assessment methodology with significantly greater focus on terrorism-related threats.

AISC has supplemented the conventional risk analysis approach with a proprietary methodology that specifically focuses on improving deterrence, detection and response capability to terrorism. The key addition to the AISC methodology is our inclusion of the offensive tactical methods employed by known terrorist organizations and counter-terrorism tactics utilized by U.S. Special Forces to properly identify organizational vulnerabilities and define proper security policies. Our ability to effectively assimilate terrorism and counter-terrorism tactics provides an innovative approach required for existing organizational security requirements.

Our corporate mission of hiring professionals – beginning with the President and CEO – who are specially trained in counter-terrorism tactics and strategic target analysis, has enabled AISC to acquire extensive knowledge of the terrorist mindset.

Our methodology enables us to identify vulnerabilities from the terrorist mindset to determine:

- Its importance and relative priority;
- Psychological or economic value;
- Attractiveness for purposes of destruction, degradation, and/or removal;
- Ease of surveillance opportunity.

The basis for this determination is the use of the **C.A.R.V.E.R.** Matrix; developed by the U.S. Special Forces and utilized by AISC operatives who served in this capacity. The C.A.R.V.E.R. Matrix is a decision tool used by U.S. Special Forces for rating the relative desirability of potential targets and for properly allocating attack resources. The C.A.R.V.E.R. selection factors of Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability assist in selecting the best targets to attack. As the factors are analyzed and values assigned, a decision matrix is formed, indicating the highest value target to be attacked within the limits of the statement of requirements.

C.A.R.V.E.R. Factors

- **Criticality**

Criticality is the importance of a system, subsystem, complex or component. A target is critical when its destruction or damage has a significant impact on the output of the target system, subsystem or complex, and, at the highest level, on the threat's ability to make or sustain attacks.

Criticality depends on several factors:

- Time. How rapidly will the impact of target destruction affect operations?
- Quantity. What percentage of output is curtailed by target destruction?
- The existence of substitutes for the output product or service.
- The number of targets and their position in the system or complex flow diagram.

- **Accessibility**

Accessibility is the ease with which a target can be reached, either physically or by standoff fire. A target is accessible when a terrorist element can physically infiltrate the target, or if the target can be hit by direct or indirect methods. Accessibility varies with the infiltration/exfiltration, survival and escape potential of the target area, the security situation enroute to and at the target, and the need for barrier penetration at the target. The use of standoff weapons such as vehicle bombs should always be considered when evaluating accessibility. Survivability of the terrorist/attacker is not always correlated to a target's accessibility.

- **Recuperability**

Recuperability is a measure of time required to replace, repair or bypass the destruction or damage inflicted on the target. Recuperability varies with the sources and ages of targeted components and with spare parts or redundant capabilities.

- **Vulnerability**

Vulnerability is a measure of the ability of the terrorist to damage the target using available assets (both persons and material.) A target is vulnerable if the terrorist has the means and expertise to successfully attack it. Vulnerability depends on:

1. The nature and construction of the target;
2. The amount of damage required/desired;
3. The assets available:
 - A. Manpower, expertise and mindset;
 - B. Transportation, weapons, explosives and equipment.

- **Effect-on-Population**

Effect-on-Population is the positive or negative influence on the population as a result of the action taken. Effect considers public reaction in the vicinity of the target, but also considers the domestic and international reaction as well. Will the attack undermine the public's confidence in the government, our economic systems, our emergency response personnel or our military?

- **Recognizability**

Recognizability is the degree to which a target can be recognized without confusion with other targets or components. Factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, and the technical sophistication and training of the attackers.

Conclusion

By assimilating conventional risk analysis, C.A.R.V.E.R methodology and an understanding of terrorist tactical methods; organizations can effectively identify and prioritize vulnerability in the Post 9-11 security environment. It is only when this task is accomplished, that an organization can attain real security and meet its fiduciary obligations to customers, shareholders and employees.

AISC is uniquely positioned to assist organizations in achieving this objective. Our proprietary analytical approach towards Vulnerability Assessments has enabled AISC to pinpoint vulnerability and develop security policy for some of the largest corporations and public agencies throughout the world. This expertise has been utilized by clients such as the Port Authority of New York & New Jersey to conduct the most complex Vulnerability Assessments ever written for non-military organizations.

About the Author

Michael Taylor is the President and CEO of American International Security Corp., which provides security services for corporations and organizations throughout the world. Prior to forming AISC, Mr. Taylor served in the U.S. Special Forces as a counter-terrorism specialist.

Mr. Taylor has been interviewed frequently by national news media on a wide range of security topics. He can be reached at 800-852-2714 to discuss the security needs of your organization.