

Protecting Students and Staff from Active Shooters

A Case Study at the European Simulation and Validation Center (ESVC)

THE TASK AT HAND – PROTECTING STUDENTS AND STAFF

Protecting the students at the European Simulation and Validation Center (ESVC) was our objective and specifically, reducing the mass casualty count during active shooter scenarios. With the increase in terrorist attack, it was only logistical that the Executive Director would seek out protection for her staff and cadre of instructors, but primarily, the students attending simulation modeling at the ESVC.

Because CPK United BV is known for their expertise in training senior government leaders and industry executives, as well as, their key staff elements, especially in the transportation and aviation fields, the ESVC is the “go to” place when it comes to conducting serious gaming models for evaluating emergency plans and the actions required by them. The ESVC provides a comfortable environment that is conducive to leadership training at the highest levels in lieu of costly field exercises. The ESVC can create an organization specific built (physical) environment virtually; use existing company or agency plans, while allowing “players” to travel down a variety of decision paths in a virtual environment. This allows them to test plans through their interaction, individually and collectively to evaluate efficiencies – without the additional expense of a full-scale exercise and without anyone getting hurt. Using ESVC simulation allows plans and procedures to be tweaked before a real incident occurs and damage or injury occur.

KNOWN COMPONENTS OF THE RISK FORMULA

All good risk formulas have some commonalities. The formula usually, goes something like this; $C \text{ (asset criticality)} \times T \text{ (Threat (What can harm us))} \times V \text{ (Vulnerability (How susceptible we are to the harm))} = R \text{ (Risk (How bad is it?))}$. In this particular instance, two of the essential elements in calculating risks were already known to the assessment team. Those elements included the **criticality of the asset**, (high value targets/students). To understand the criticality, imagine for a second, if a multi-national corporation’s entire senior leadership along with key staff were on-site being trained and ESVC were involved in a catastrophic incident. It would not only mean damage and death but could also influence the future of the organization and could very well be the end of that company.

And, the second known element – threat – was an **active shooter** scenario.

ASSESSING VULNERABILITIES – A SNAPSHOT IN TIME

The next element of the formula was to determine the vulnerabilities of the site as they related to the threat. Haines Security Solutions was called in to do the assessment due to its extensive experience in conducting risk analysis and developing mitigation strategies as they relate to building design. Experts in forced entry, building design, antiterrorism and structural engineering repaired to the site to conduct the evaluation.

It should be noted that during conversations with the staff it was noted there was a low-moderate probability of occurrence of this type of attack; however, due to the catastrophic impact on the corporate structure of an organization attending training if impacted (low/moderate risk – critically high impact), it was determined to be of extremely high importance to conduct a full range of assessments.

Each area of the facility (reception area, training facility, staff offices, storage areas, coffee/snack center, bathrooms and print shop) was examined from both the owner's and the aggressor's points of view.

USING THE ASSET BASED RISK ANALYSIS METHODOLOGY

This dedicated team of subject matter experts collected physical security, as well as, operational data on-site in order to allow them to fill-in the vulnerability element and complete the risk formula

They then started collecting physical data from the curb inward. Data was collect on three layers where vulnerabilities could occur; i.e., property perimeter, building façade and internally controlled spaces. Data about the IT system or software used at the ESVC was not collected because the ABRA, in this case, did not call for the protection of data on the IT system. Instead, it called for the protection of lives.

Once back at their offices, the Haines Security Solutions team members used an assessment methodology called Asset Based Risk Analysis or ABRA to analyze the data and make effective recommendations.

The primary purpose of ABRA is to quantitatively measure threats, assets, vulnerabilities, and risks associated with large and/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, ABRA 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, ABRA identifies the associated cost and impact of the improvements. ABRA includes the performance of six sub-analyses: threat, target, vulnerability, optimization, risk, and cost–benefit.

Threat Analysis

The treat analysis is based on information collected during the site visit. The information produces a threat rating, which measures the threat likelihood (the probability an attack will occur), and an effectiveness rating (the probability that an attack will be successful).

ABRA takes into account the current local threat environment for five conditions; i.e., stand-off, explosive; covert, overt and chem/bio. Although the project only called for the assessment of an active shooter threat, since we were already on site, it only made sense to conduct all five analyses.

The assessment team started the assessment asking a series of about 50 questions to the staff to further determine the asset's criticality and threat environment. Additional soft intelligence was collected via the internet and a clear threat picture emerged.

Target Analysis

The target analysis is designed to evaluate and measure the value of all targets to the user and 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.

Vulnerability Analysis

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

Optimization Analysis

The 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, in this case, a training facility. Based on the optimization analysis, the average vulnerability and risk rating can be identified and stated as a percentage.

Risk Analysis

The risk analysis is the aggregation of the threat, target, vulnerability, and optimization analyses to determine the calculated value of risk associated with a specific asset that is being targeted by a specific threat.

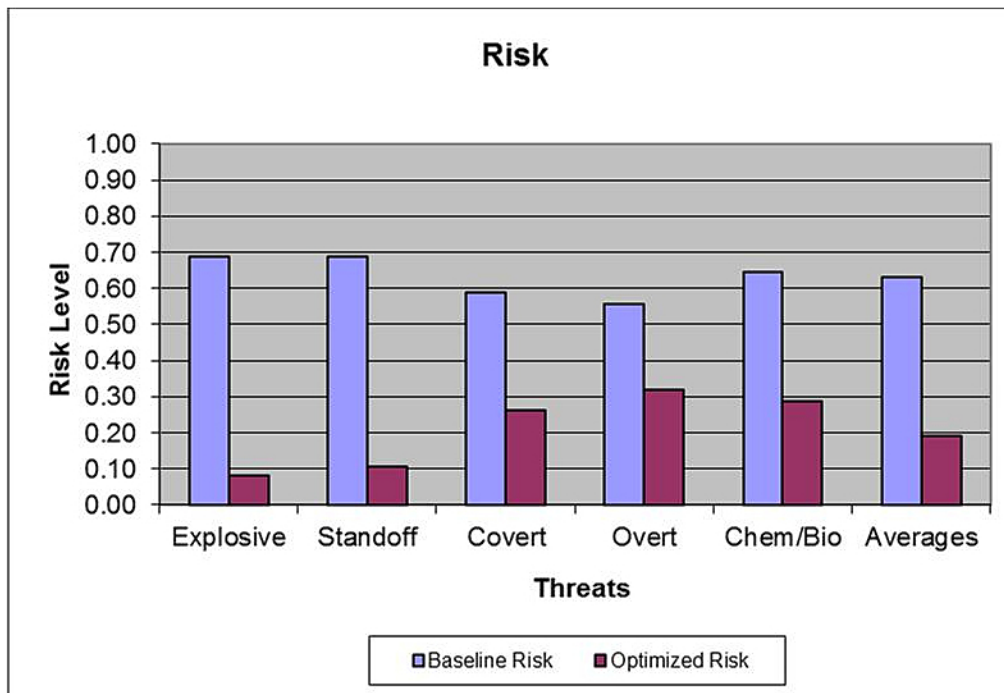


Chart showing baseline (Snapshot in time) and optimized (after recommendations are implemented) risks.

Cost-Benefit Analysis

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

MAKING RECOMMENDATIONS THAT WORK

Most risk analyst make recommendations that bring the facility up to code compliance or base solutions on costs. The recommendations made during this assessment were made based on risk reduction and not costs. Our analysis showed that all recommendations were either extremely or highly cost effective. Those recommendations included four main or specific areas.

Inhabited Space Hardening

Windows – Replacing the existing exterior windows with 6 mm laminated or poly-bicarbonate glazing.

Walls – Retrofitting the walls with a ballistic resistant material and continuing that concept to other features.

Furniture – Retrofit any interior elements, such as, reception desk, student chairs, tables, white-board (basically, anything or anywhere a student could hide behind if they were unable to exercise their first option of running away).



A wide-array of ballistic protection applications. Courtesy Amulet® Protective Technologies.

Electronic Security Systems

Electronic Security Systems – Install integrated access control and surveillance (CCTV) systems.

Mass notification system – Install internal and external speakers, alarm signals and visual message boards.

Crime Prevention through Environmental Design (CPTED)

Natural Surveillance/Natural Access Control – Use landscaping to reroute pedestrian traffic entering the building, so that as people approach they are observed from within the building.

Plans, Policies and Procedures

Use internal resources/corporate expertise to update plans, policies and procedures

IN SUMMARY

The recommendations would be implemented in all areas of high occupancy or critical areas (inhabited spaces); i.e., training facility, staff offices, coffee/snack center and stairway. It should be pointed out that normally stairways or other transit type spaces would not receive the same level of protection because they are usually considered to have low occupancy, but input from the ESVS indicated it to be mission critical and a single-point-failure location for their operations.

Bathrooms, storage rooms, print shop and garage were not recommended to be retrofitted with ballistic protection because of their low occupancy density (uninhabited spaces).

Overall the risk reduction to the active shooter threat was calculated at 84 percent. In other words, the Delta if you will, from where the risk is today to where it will be when all of the recommendations are implemented. If implementation of all of the recommendation in the report were accomplished the risk reduction of the other threat scenarios would be between 74 and 98 percent. The total project costs, including the data collection, evaluation and analysis and implementation of all of the recommendations was Euro72,130 (\$76,200). If only the recommendations pertaining to ballistic protection from the shooting threat were adopted the costs would be Euro53,560 (\$56,700). Recommendations were also prioritized to be implemented based on risk reduction and protection to the largest number of people first, and to allow their implementation as funding becomes available.

In summary, that's a very small amount to pay to protect the lives of students and staff. The added protections afforded by the recommendations help reduce risk and provide safety from a host of criminal and terrorist activities. Making it a safe and secure environment for those attending training – after all isn't that what it's all about?