Small arms attack on a Pacific Gas and Electric Company substation south of San Jose, California in April 2013 (Photo courtesy of RLM News)

Newsletter #1:
Security Risk Management at a Facility or Vessel

Applying probabilistic risk analysis to individual targets

Jeffrey Fuller, President Security Risk, Inc.
4003 Hunting Pines Ct. Fairfax, VA 22032
M: (571) 244-3638 E: info@securityriskinc.com
March 2014

Dear Newsletter Subscriber:

This newsletter provides an overview of the concept we recommend to understand and apply the threat analysis and to determine the most cost effective strategies to manage prioritized threats for a single facility of vessel.

Regards,

Jeff Fuller
Why bother with risk-based security management?

Almost any significant infrastructure and key facility or vessel fleet in the United States expends resources on security. The annual investment in security planning, training, exercises, and day-to-day execution is often best described as a legacy program, processes, and activities that have evolved over time. Corporate and government financial pressures demand more for less. Legal and moral obligations to protect employees and materiel, as well as those who may be impacted beyond the facility, infrastructure, or vessel also weigh on leaders.

So, the basic question: “Is our security program delivering effective return-on-investment (ROI) considering risk reduction and cost?” (Figure 1)

In other words, can we measure the effectiveness of our security program? Can we adjust plans, procedures, and security measures to achieve improved return-on-investment? This question applies to large institutions and to operators of facilities, infrastructure, or vessels.

The answer is yes. For large operations like the US Coast Guard (USCG), this is a daunting problem as there are thousands of prospective targets spread across the nation’s ports and waterways. For an important facility operation or vessel, the same probabilistic risk theory is applied as it is for the Department of Homeland Security (DHS) and USCG terrorism risk management programs.

Since 9/11, the United States Coast Guard (USCG) has conducted an aggressive terrorist risk analysis and management program focused on direct and exploitation attacks. This program is known as the Maritime Security Risk Analysis Model (MSRAM). The MSRAM methodology and supporting software tool are used to identify, characterize, and quantify risks from terrorist threats. These threats consist of potential attacks carried out on targets, on or near national coasts and waterways by archetypal attack modes, such as boat bombs, assault teams, ramming by hijacked vessels, and weapons of mass destruction (WMD).

To execute MSRAM across the nation USCG has developed a rigorous analytic method, with a sophisticated threat analysis model, a robust process of consequence and vulnerability data collection, analysis, and review. Furthermore, USCG has supporting risk management tools and data analysis to support risk-based policy, resources allocation, and day-to-day operations.

The concept outlined below, is how a facility or vessel operator can apply the risk analysis concept the US Government uses, with the appropriate level of detail and sophistication.

---

1 The Department of Homeland Security (DHS) has produced a Risk Management Fundamentals doctrine, which asserts that Risk is a function of threat (T), vulnerability (V), and consequence (C). Consistent with this definition, MSRAM applies a Probabilistic Risk Assessment (PRA) approach to compute the relative risk of terrorist maritime threats as a product of estimated T, V, and C.
## Risk-Based Security Management Concept

The concept is to employ a collaborative approach to develop strategies to manage risk of terrorism, criminal activity, cyber, and insider threats. This requires three sequential risk analysis and management steps (see Figure 1):

1) **Threat Analysis**: Identify and weigh the threats challenging your organization.

2) **Risk Analysis**: Analyze the consequences of these threats and associated vulnerabilities given the current security program.

3) **Risk Management**: Consider risk mitigation strategies that either reduce vulnerabilities, consequences, or both, or estimate costs for a rough return-on-investment for each strategy.

### Collaborative Approach

It has been our experience that the quality of the data is improved when a number of participants with 'skin in the game' are involved. That is, include the leadership, operations staff, security staff, and law enforcement agencies with a role in detecting and interdicting the threat.

Regardless of how effective the security team is at risk analysis, unless leadership is on board from the start, there is a high risk that the proposed changes will not resonate. Leaders must have an appreciation of the method and processes, and be involved at key steps to achieve changes that significantly improve security based on ROI. It is also important to include facility / vessel operations staff, since changes in security may impact their operations. They need to have been at the table to contribute to the analysis, and have an understanding of the underlying rationale for the recommended risk management strategies. In many cases, facilities and vessel security staff rely exclusively on law enforcement agencies (LEA) to interdict the threat. LEAs are usually willing to contribute to a risk analysis as they can provide input on the threats and can gain insight into a prospective attack at a facility or vessel in their area. If the risk analysis reveals significant risks, they may be willing to participate on combined planning and as a risk mitigation measure.

Finally, in cases where a threat scenario poses a significant risk, we recommend a combined system security plan and exercise program. This strategy can have significant payoff at modest cost.

### Conclusion

#### Outcomes

*The bottom line should be a better focus of security resources, procedures, materiel, and a case to present to your insurance carrier to seek reduced insurance rates.*

If a facility or vessel owner goes through the three risk-management steps described above, the following outcomes will be an indication of a successful project:

1) Shared vision of the threat by leaders, operators, security team (and LEA)

2) An accepted picture of the baseline risk, represented by relative risk scores.
3) If the baseline risk is not acceptable, a list of risk management strategies ranked by ROI, as well as a risk management plan with milestones, costs and savings, if required.

**Project Risk Mitigation**

Not all owner/operators and their teams are able to execute the risk management approach described above. To enhance the chance for success, owners and their team should consider conducting a security risk management seminar.