Security Risk Assessments: Integrating the Concept

By William J. Malampy and John W. Piper

During 2006, the authors of this column were requested to execute a security risk assessment at a major liquefied natural gas facility in the Asia-Pacific region. The provincial government had ordered that significant capital projects required a security risk assessment be conducted as part of their Environmental Impact Statement (EIS) requirements — otherwise, no permits for construction would be issued.

It is interesting to note that this method — a security risk assessment in the context of an EIS — has yet to be adopted in the United States; however, the concept has garnered interest among individual security professionals in the public and critical infrastructure sectors. It goes by a slightly different title: Security Impact Assessment (SIA). This SIA was originally developed and published as a proposed solution to many government security problems in 2006 by the Center on Terrorism & Counter-Terrorism at the Foreign Policy Research Institute in Philadelphia, under the direction of Professor Stephen Gale.

The Security Impact Assessment concept was crafted to provide a clear standard for measuring and assessing the operational and financial value-add of investments made in security. These measures would provide organizations such as the DHS with a clear measuring stick of the relative financial benefits associated with considering alternative security investment strategies. According to *"From MAD (Mutual Assured Destruction) to MUD (Multilateral Unconstrained Disruption): Dealing with the New Terrorism"* by Stephen Gale and Lawrence Husick (http://www.fpri.org/fpriwire/1101.200302.galehusick.madtomud.html), the SIA should provide, at minimum, an assessment and description of the following:

- The impacts on security of both the proposed action and the failure to act;
- Any adverse security effects that would be avoided should the proposal be implemented, as well as those that are unavoidable;
- Alternatives to the proposed action, the expected criteria for decision making, and analysis of why the proposed action is preferred under those criteria;
- The costs of the proposed action (including the expected costs to the nation as a whole) of a successful attack, and an estimate of the net current value of the investment required to take the proposed action; and
- An estimate of the expenditures involved in implementing the proposed action.

As envisioned by its creators, the Security Impact Assessment would use a Value-Added Model for Security Management (VAM) to provide quantitative estimates of the likelihood of undesirable events and the impact of risk mitigation measures. VAM provides a financial measurement of the relative value added of security — which could drive security investment — rather than simply emphasizing cost reduction and the financial consequences of events.

As we have seen in America with the Chemical Facility Anti-terrorism Standards (CFATS), there are a variety of constraints associated with setting specific security objectives for critical infrastructure sectors. A combination of Security Impact Assessment objectives with something similar to EPA's EIS techniques, however, should enable a level of consideration of individual facilities' unique situations that broad legislative standards often do not.

The Security Impact Assessment would use a Value-Added Model for Security Management (VAM) to provide quantitative estimates of the likelihood of undesirable events and the impact of risk mitigation measures.

Nothing has yet come of the Security Impact Assessment initiative here in the United States. The Asia-Pacific countries have embraced the concept wholeheartedly, and some have even codified it as part of their laws. If the United States adopted a Security Impact Assessment requirement, security would be guaranteed the right seat at the right table, at the right time. Security would also have the opportunity to set specific goals that can be worked into project management systems, and the results aligned with many other organizational requirements. This would avoid security surprises as well as expensive technical and procedural retrofits during construction. Finally, a Security Impact Assessment would allow the baseline measures at the permit phase to be well understood, creating a better overall security environment.

In the Asia-Pacific test case, the Security Impact Assessment improved security, safety and management — clearly a better value for investors, taxpayers and the government. The U.S. government should follow suit.

• William J. Malampy is the Deputy Director of the Center on Terrorism & Counter-Terrorism (CT&CT) at the Foreign Policy Research Institute in Philadelphia, PA. He is also a Senior Fellow at the CT&CT.

• John Piper is a member of the faculty of the Security Executive Council and former manager of global security engineering and risk management for ExxonMobil Corp., as well as a Senior Fellow for FPRI.

• The Security Executive Council (www.securityexecutivecouncil.com) is an innovative problem-solving research and services organization that works with Tier 1 Security Leaders to reduce risk and add to corporate profitability in the process.Through its pioneering approach of Collective Knowledge, the Council serves all aspects of the security community. To learn about becoming involved, e-mail contact@secleader.com.