

Security Vulnerability Analysis



More than a Suggestion

Several organizations are requiring members to perform security vulnerability analyses. Are you a member of one of these?

- American Chemistry Council
- Synthetic Chemical Manufacturers Association
- American Petroleum Institute
- The Fertilizer Institute

Pending federal legislation would require identification of high-risk facilities that will have to complete vulnerability analyses, prepare response plans, and implement security measures. In addition, the USEPA supports legislation requiring all facilities that prepare risk management plans to complete security vulnerability analyses as well.

Regardless of federal legislation or trade organization affiliation, some companies are voluntarily conducting SVAs for business risk-management reasons.

Assessing the Potential for Intentional Harm

You probably don't like to imagine the unimaginable occurring at your facility. But to avoid thinking about the unthinkable—the potential for intentional harm involving chemicals at your facility—could be irresponsible. Assessing your facility's vulnerability now and developing countermeasures and security precautions *before* something happens can greatly reduce the risk of being taken by surprise.

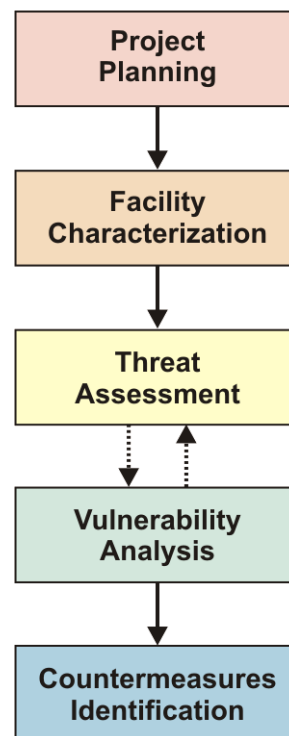
The Center for Chemical Process Safety (CCPS) has published guidelines to use in addressing the potential for intentional acts against facilities that use or store hazardous chemicals. The CCPS, along with the American Chemistry Council and the Synthetic Organic Chemical Manufacturers Association, recommends a five-step process for conducting a security vulnerability analysis (SVA).

Where to Begin?

In the **project planning** phase, an SVA team is assembled that includes not only experts in SVA procedures and process safety management but also those with expertise related specifically to facility operations and processes.

In the **facility characterization** phase, the SVA team identifies critical chemicals at the facility and the hazards associated with damage to or loss of these. The team also analyzes the attractiveness of these chemicals as possible targets and the level of protection currently securing them. Ultimately, they must also determine the consequences to the facility, the business, and the surrounding community if these chemicals were to be compromised.

The **threat assessment** phase of the analysis is intended to identify and characterize potential adversaries. Often, the SVA team coordinates its efforts with those of local police and public safety agencies, as well as state and federal law enforcement agencies. Sometimes, outside security consultants are brought in.



(Continued)

Under lock and key . . .

The information used to conduct an SVA and the information resulting from one must be kept confidential. In the wrong hands, this information could be misused—with disastrous consequences. It's essential to make plans for controlling and safeguarding this information before the SVA process even begins.

(SVA phases, continued)

The **vulnerability analysis** phase takes the assets identified in the characterization phase and the threats/adversaries identified in the assessment phase and pairs them, developing a matrix to help evaluate the likelihood of an attack and its consequences. Using this, various scenarios (pairings of assets and threats) can be ranked. Those scenarios that pose an unacceptably high level of risk can be investigated early on to determine possible precautions and countermeasures.

The final phase of the SVA involves **identification of countermeasures** to defend against potential attacks and reduce the risk associated with identified scenarios. The SVA team may rely on the company's protection performance standard to develop criteria, or it may brainstorm ways to either increase the facility's level of protection or reduce the attractiveness of possible targets.

At the conclusion of the security vulnerability analysis, the facility should have both a list of potentially vulnerable security concerns and recommendations for reducing the risk associated with these.



For information on the full range of Barr's engineering and environmental services, visit www.barr.com

Barr Can Help You Be Prepared

Barr's team of process-safety and risk-management specialists includes staff certified by CCPS to conduct security vulnerability analyses. Their work for clients dealing with hazardous materials, chemicals, and petroleum products will enable them to help your staff identify and prioritize security concerns. Turn to Barr when you need help:

- Determining whether your facility needs to perform an SVA
- Setting up an SVA team
- Identifying potential chemical targets and potential adversaries
- Conducting a vulnerability analysis
- Characterizing protective countermeasures
- Prioritizing risk-reduction efforts

For more information on security vulnerability analyses and how Barr's SVA specialists can help you, contact Joel Trinkle at 952-832-2870 (jtrinkle@barr.com) or Catherine Meuwissen at 734-327-1200, extension 1204 (cmeuwissen@barr.com).