SYSTEM SECURITY RISK ANALYSIS

M. Borysiewicz
Institute of Atomic Energy

The industry and operators of various element of critical infrastructure face the important need to assess whether current security measures effectively address the new and unforeseen threats, and make enhancements as required to provide for the safety of the public, workers, and the environment. Security risk management involves the systematic identification, analysis, treatment (e.g., mitigation, acceptance, transfer), monitoring, and communication of risk. Key components of a security risk management process are risk analysis, in which a system, its components, and their relationships are analyzed with respect to threats and vulnerabilities; risk assessment, in which the level of risk is determined based on analysis and a well-defined approach to identifying and assigning values to risk factors, including possible consequences or impacts of threats; and risk communication, in which the results of a risk assessment are translated into terms that are meaningful to decision-makers.

Security incidents are intentional, rather than accidental, which is a key basis to understanding the hazards, likelihood, and possible consequences. The risk that is being analyzed to solve security issues is an expression of the likelihood that a defined threat will reach a specific vulnerability of a particular attractive target or combination of targets to cause a given set of consequences.

The estimate of consequences may be different in magnitude or scope than is normally anticipated for accidental releases. In the case of security events, adversaries are determined (sometimes at all costs) to find vulnerabilities and to maximize damage. In addition, theft or diversion of chemicals is normally not considered in accidental release studies, but should be included in security studies.

A second unique term of interest is vulnerability, which is any weakness that can be exploited by an adversary to gain unauthorized access to an asset. Vulnerabilities can result from, but are not limited to, management practices, physical security weaknesses, or operational factors.

A variety of approaches to system security risk analysis and risk assessment have been taken:

Policy-based approaches focus on security requirements, as stated in organizational Policy documents, or in applicable regulations or standards. Failure to meet a requirement – typically, to implement a specific safeguard – constitutes a potential source of risk. In a policy-based approach, the consequences of such a failure are analyzed and assessed.

Threat-based approaches focus on how an adversary could exploit technical aspects of a system (e.g., inherent vulnerabilities, poor configuration of key components), as well as non-technical aspects of the system's operational environment, to produce adverse effects. Analysis, rather than assessment, predominates in a threat-based approach.

Asset-based approaches focus on the assets that must be protected from threats. An asset-based approach includes identification of system components, as well as analysis of their interconnections and dependencies.

Mission- or objective-based approaches focus on the missions or business objectives that must be achieved, despite the presence of threats. A mission-based approach includes identification of business functions and how those functions relate to (e.g., depend upon, impose requirements on) systems and their behavior.

The an analytical portion of these approaches is called a Security Vulnerability Analysis (SVA). The leading institutions and organizations (e.g. Center for Chemical Process Safety - CCPS) dealing with chemical process safety) created the SVA methodology to help companies to evaluate the vulnerability of their chemical sites to terrorist attack or other malicious acts. Methods available to SVAs can have varying scopes, varying levels of detail, and utilize different methods.

The SVA approach can also applied to information/cyber security, where the objective of is to protect critical information systems including hardware, software, infrastructure, and data from loss, theft, or damage. In a chemical facility, protecting information and computer networks means more than safeguarding a company's proprietary information and keeping the business running, as important as those goals are. It also means protecting chemical processes from hazardous disruptions and preventing unwanted chemical releases. To an adversary, information and network access can provide the power to harm the company, its employees, and the community at large.

A analysis of SVA methodologies and approaches to SVA based security management in chemical process industry, the related information/cyber security and Industrial Control System were studied by the author, in the framework of the project on integrated methods for major accidents . risk and security implement in the period 2005- 2007 by the Central Institute of Labour Protection n Warsaw