SCREENING FACILITIES FOR CYBER SECURITY RISK ANALYSIS

by Paul Baybutt
Primatech Inc.
paulb@primatech.com
614-841-9800
www.primatech.com

Abstract

Many chemical companies have performed security vulnerability analyses (SVAs) for their facilities since the middle of 2002 when the American Chemistry Council issued a new Security Code of Management Practice and required its member companies to follow it. The first step was to prioritize facilities for analysis using a simple screening scheme. These initial SVAs have focused on physical and personnel security and usually have not explicitly addressed cyber security. It is expected these SVAs will soon be extended to address cyber security. This paper provides a modification of the ACC screening scheme that can be applied to cyber security.

Keywords: Terrorism, cyber security, risk analysis, vulnerability analysis, threat analysis, risk screening.

Introduction

Security Risk Analysis (SRA), also called Security Vulnerability Analysis (SVA) addresses malevents such as terrorism, sabotage, and other criminal acts in process plants [1-4]. Malevents are deliberate acts that result in adverse consequences. They are to security what accidents are to safety. Since the events of September 11, 2001, the chemical process industries have invested considerable effort in this area. Initial attention has been focused on physical and personnel security. Very little attention has been paid to cyber security for industrial processes[5].

Physical security addresses protection measures such as fencing, vehicle barriers, area lighting, surveillance systems, guards and dogs, intrusion detection systems, and access controls. *Personnel security* addresses protection measures such as screening and controlling personnel, maintaining good labor relations, and taking appropriate actions on termination. *Industrial cyber security* addresses the protection of manufacturing and process control computer systems, and their support systems, from threats of cyber or physical attack by adversaries who wish to disable or manipulate them to cause harm, or access by adversaries who want to obtain, corrupt, damage,

destroy or prohibit access to valuable information.

Member companies of the American Chemistry Council (ACC) are required to comply with the Responsible Care® Code of Management Practices, including the Security Code[6], and have already performed SVAs for many of their facilities. Cyber security has not usually been addressed explicitly in this first round of analyses. However, the ACC will require these facilities to address cyber security. The initial SVAs were prioritized and assigned to tiers with different deadlines established. This prioritization may not necessarily be appropriate for cyber SVAs at these facilities. Therefore, a separate prioritization of a facility's computer systems should be performed. This paper describes an approach for performing such a screening study.

Risk-Based Screening

The objective of risk-based screening is to produce a list of facilities prioritized in the same order as would be obtained by performing detailed risk analyses but to do so quickly and easily. This was accomplished by ACC member companies for initial SVAs by using a simple rating scheme[6] for facilities and processes covered under Program 2 or 3 of EPA's Risk Management Program (RMP) regulations, 40 CFR Part 68. The scheme was based on the relative Difficulty of Attack (D), Severity of Attack (S) and Attractiveness of the Target (A). These three factors were rated on a four-point scale for a security worst-case scenario based on the RMP worst-case scenario for the process and added together to produce a Security Risk Index (SRI). For facilities with more than one RMP process, the highest SRI for an individual process was used as the overall facility SRI. Using this SRI, the facility was assigned to one of four tiers that defined the deadline for completing the initial SVAs.

The four-point scale for Difficulty of Attack was defined in terms of the amount of planning, coordination, knowledge/training and equipment needed; the number of people required; and the need for access to restricted areas (number of independent security protection layers that must be breached). The scale for Severity of Attack was defined in terms of the population within the area affected by the attack. Both toxic release and fire scenarios were considered. The Attractiveness of the Target was defined in terms of the extent of disruption likely (local, community, regional, national). This scheme effectively provides a risk ranking as can be seen by considering the risk of a malevent which is evaluated as:

Risk = S (Malevent) x L (Malevent)

where: S (Malevent) = the severity of the malevent which depends on the type and magnitude of the consequences, and

L (Malevent) = L (Attack) x L (Success) where:

L (Attack) = the likelihood of attack which depends on the attractiveness of the target and the motivation, capabilities and intent of adversaries, and

L (Success) = the likelihood of success which depends on the vulnerabilities present (i.e. failure or defeat of countermeasures) and the characteristics and tactics of the assailants.

These elements of the risk calculation correlate with the elements of the ACC scheme as follows. The Difficulty (actually *Ease*) of Attack approximates L (Success), Severity of Attack is the same as S (Malevent), and Attractiveness of the Target approximates L (Attack).

There are many different types of consequences possible for a malevent. The ACC scheme uses the *affected population* as a reasonable surrogate for consequences. There are also many factors that affect the Attractiveness of the Target. The ACC scheme again uses a single facility attribute, the *extent of disruption*, as a surrogate for other attractiveness factors. This is based on the assumption that the extent of disruption represents the dominant contributors to Attractiveness of the Target.

Risk-Based Screening for Computer Systems

Ideally, a scheme is needed to prioritize a facility's computer systems that approximates the ACC scheme that is already familiar to many of the companies who will be performing cyber SVAs. The same risk-based model that rates the relative Ease of Attack, Severity of Attack, and Attractiveness of the Target can be used for this prioritization.

Attractiveness of the Target for Computer Systems

Using the *extent of disruption* employed in the ACC scheme as a surrogate for the factors that influence the Attractiveness of the Target may not be a reasonable assumption for cyber attacks. They are most likely to occur when attackers identify a target computer system to attack rather than choosing a facility based on the impact that can be created, and then figuring out a way to attack it by cyber means. Consequently, the following scheme that considers the ease of target identification can be used for rating computer systems based on Attractiveness of the Target:

Description and factors which influence the Attractiveness of the Target for computer systems	
1	The company has a low profile. There is protection against scanning. Precautions are taken against war dialing.
2	Vulnerability scanning and war dialing are performed as part of network management.
3	No precautions taken against wardriving. Company web sites provide information useful for a cyber attack. Information on hardware and software used is readily available from vendors.
4	The company is well-known. Dial-up modems use the same block of lines as telephones. Company telephone directories can be obtained by outsiders. Personnel may be susceptible to social engineering. Sensitive trash is not shredded or incinerated.

Severity of Attack on Computer Systems

Using the population potentially affected as a surrogate for consequences as in the ACC scheme is also appropriate when considering industrial cyber threats. However, one difficulty is that the RMP worst-case and alternative release scenarios are not necessarily appropriate as cyber attack scenarios. A worst-case cyber attack scenario must be selected, and if its consequences do not approximate those of the RMP worst-case scenario, alternative methods should be used to estimate the consequences. The Center for Chemical Process Safety (CCPS) has presented methods that can be used for non-RMP processes or for scenarios not considered in RMPs[(2)].

Alternatively, a generic scheme can be used with the following ratings:

Description and factors which influence the Severity of Attack for computer systems	
1	Impacts confined to the facility
2	Impacts confined to the community
3	Impacts confined to the region
4	National impacts

Ease of Attack on Computer Systems

Ease of Attack for cyber systems will be determined largely by the ease of penetration of the computer system. The following ratings and guidelines can be used for Ease of Attack for computer systems:

	Description and factors which influence the Ease of Attack for computer systems
1	The process control network is isolated. Strong passwords or other forms of authentication are used. Computer systems are physically protected. Malware has not been a problem. There is a program to manage software patches.
2	The process control network is provided with firewall and DMZ protection and encryption is used. There is an intrusion detection system and sniffing countermeasures. The facility has a cyber security management program.
3	Workstations on the process control network have Internet access. The system contains secured modems. Workstations are left unattended and unsecured. Multiple networks are connected to the process control network. There is no program to educate users on cyber security. Portable PCs are used at home and work.
4	Computer systems contain unsecured dial-up modems. Wireless networks are used without security features enabled. Weak passwords/poor password management. Computer systems lack physical protection. There is a history of malware on facility computer systems. Software patches are usually not installed.

Alternatively, a set of standard cyber vulnerabilities can be defined, and each computer system rated on a scale of 1 (least vulnerable) to 4 (most vulnerable) for each vulnerability. The individual vulnerabilities can then be combined, using weighting if desired, and normalized to lie in the range of 1 - 4 so they can be combined with the other two ratings factors to produce an SRI for the computer system.

Example of Cyber Security Screening

A distributed computer control system (DCS) is used in a chemical plant to control a process using multiple reactors. One of the reactions is susceptible to runaway if the

temperature is not carefully controlled. Process control set points can be changed from a workstation in the control room. The workstation has a dial-up modem so the process engineer can troubleshoot the process from home. Access is password protected but there is no company password policy. The engineering workstation has a hard-wired connection to a separate computer system that operates safety instrumented systems for the process. In the event of a runway reaction, there would be a large release of a highly toxic chemical that would have significant impacts on the population surrounding the plant. The company is well known and there are few precautions taken to limit the availability of information available to an attacker.

For this computer system, ratings are assigned as follows:

Factor	Rating	Comments
Ease of Attack	4	It will be fairly easy to identify the modem on the workstation by war dialing.
Severity of Attack	2	Impacts will be confined to the community.
Attractiveness of the Target	4	It is hard to decide if the rating should be 3 or 4. It is rated as 4 to be conservative. The dial-up modem is probably protected with a weak password and it provides access to both the computer control and safety systems. Information is readily available on the equipment and software used and a skilled attacker may be able to manipulate the process to cause a runway reaction.

The Security Risk Index for the computer system is the sum of the ratings for the factors in the table, i.e. 10. In the original ACC scheme, ratings were used to assign facilities to tiers are follows:

SRI	3	4	5	6	7	8	9	10	11	12
Tier	. 4	3	3	3	2	2	2	1	1	1

Deadlines were established for each tier with the completion of SVAs for Tier 1 facilities required first. If similar tiers are used for cyber security, the computer system in the example would be assigned to Tier 1 and require attention first.

Conclusions

A modification of the ACC method for screening facilities for the performance of cyber SVAs has been described. It uses the framework of the original scheme but provides screening criteria more appropriate for cyber threats. Its application to computer systems is very similar to the application of the original scheme for processes in facilities.

References

1. Sandia National Laboratories, www.sandia.gov

2. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, August 2002, Center for Chemical Process Safety.

3. P. Baybutt, Assessing Risks from Threats to Process Plants: Threat and Vulnerability Analysis, Process Safety Progress, p. 21, No. 4, December, 2002.

4. P. Baybutt, “Security Risk Analysis: Protecting Process Plants from Terrorism and Other Criminal Acts”, submitted for publication, 2003.

5. P. Baybutt, “Making Sense of Cyber Security”, submitted for publication, 2003.

6. Implementation Guide for Responsible Care® Security Code of Management Practices, Site Security and Verification, American Chemistry Council, July 2002.