INTEGRATING AND IMPROVING CYBER AND PHYSICAL SECURITY VULNERABILITY ANALYSIS (SVA)

by Paul Baybutt, Primatech Inc.

Presented at the

1st Latin American Process Safety Conference and Exposition,

Center for Chemical Process Safety, Buenos Aires, May 27 – 29, 2008

paulb@primatech.com

www.primatech.com

OVERVIEW

- Background
- Cyber security
- Security Vulnerability Analysis (SVA)
- Integration and improvement of cyber and physical SVA
- Lessons learned
- Conclusions

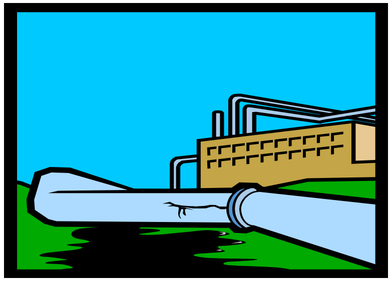
BACKGROUND

> “There are many ways of going forward, but only one way of standing still.”
>
> Franklin D. Roosevelt

EXTRAORDINARY EVENTS

PHA

Accidents

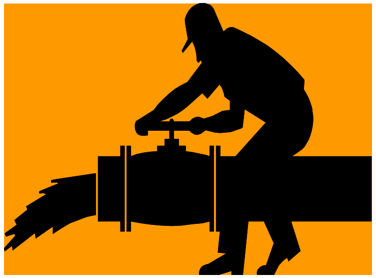


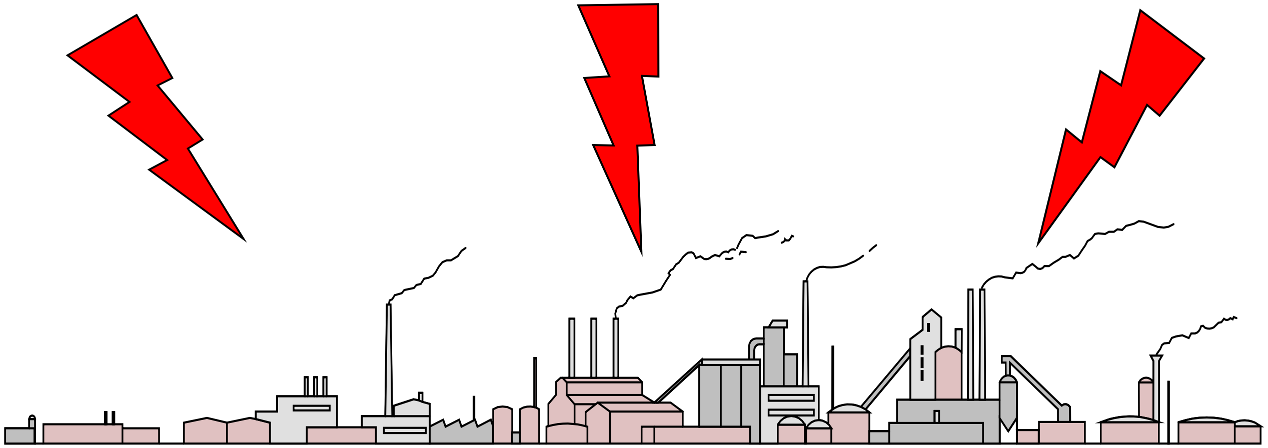
PHA and ERP

Natural Events

SVA

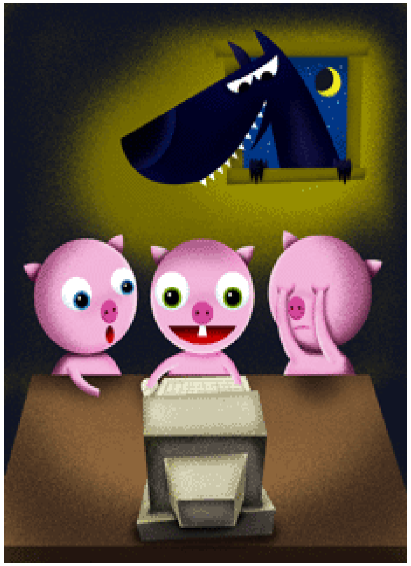
Malevents (Deliberate Acts)





MALEVENT THREATS

- Physical
- Cyber



PHYSICAL SECURITY PROTECTS AGAINST THREATS OF…

- Release of hazardous materials
- Theft or diversion of materials
- Contamination of chemicals, materials or products
- Damaging, destroying or stealing assets
- Manipulating or disabling equipment, processes, plants or other assets

CYBER SECURITY PROTECTS AGAINST THREATS OF…

- Cyber attack to disable or manipulate computer systems
- Physical attack to disable or manipulate computer systems
- Access by adversaries who want to obtain, corrupt, damage, destroy or prohibit access to valuable information

SOURCES OF THREATS

- Internal
  - E.g. Disgruntled employees or contractors
- External
  - E.g. Terrorists, criminals, activists, hostile governments

EXAMPLE – PHYSICAL ATTACK ON A CHEMICAL FACILITY

- In 1997, four KKK members plotted to place an improvised explosive device on a hydrogen sulfide tank at a refinery near Dallas
- FBI infiltrated the group

EXAMPLE - CYBER ATTACK ON A WASTE-TREATMENT PLANT

- Disgruntled contractor caused the release of millions of gallons of raw sewage in Queensland, Australia

WHAT IS THE CURRENT STATUS OF SECURITY IN PROCESS PLANTS?

- In 1999, the Agency for Toxic Substances and Disease Registry (ATSDR) reported that
  - "Security at chemical plants ranged from fair to very poor"
  - "Most security gaps were the result of complacency and lack of awareness of the threat"
- US industry and government have acted, e.g.
  - ACC Security Code, 2002
  - DHS CFATS Regulation, 2007

POSSIBLE APPROACHES FOR PROCESS SECURITY

- Head in the sand
- Reactive
- Proactive

“What we anticipate seldom occurs; what we least expected generally happens.” Benjamin Disraeli

CYBER SECURITY

> "Most human beings have an almost infinite capacity for taking things for granted."
>
> Aldous Huxley

CYBER VULNERABILITIES

- Control systems are increasingly connected to business, commercial and enterprise networks
  - These are connected to the Internet
- Control systems may also contain:
  - Computers with Internet connections
  - Modems for remote access

CYBER VULNERABILITIES (CONTD.)

- Current control systems:
  - Not designed with public access in mind
  - Often have poor security
- Much of the technical information needed to penetrate these systems is readily available

CYBER THREATS ARE REAL

- In 2003 the Slammer worm was released (malware)
  - Utility's SCADA network was downed when Slammer moved from a corporate network to the control center network
  - Some petrochemical plants lost HMIs and data historians
  - In Ohio's Davis-Besse nuclear power plant a safety monitoring system was disabled
    - Despite a belief that the network was protected by a firewall
    - Event occurred due to an unprotected interconnection between plant and corporate networks
- These were the effects of the release of one *unintelligent* piece of malicious software
  - No specific facility was targeted

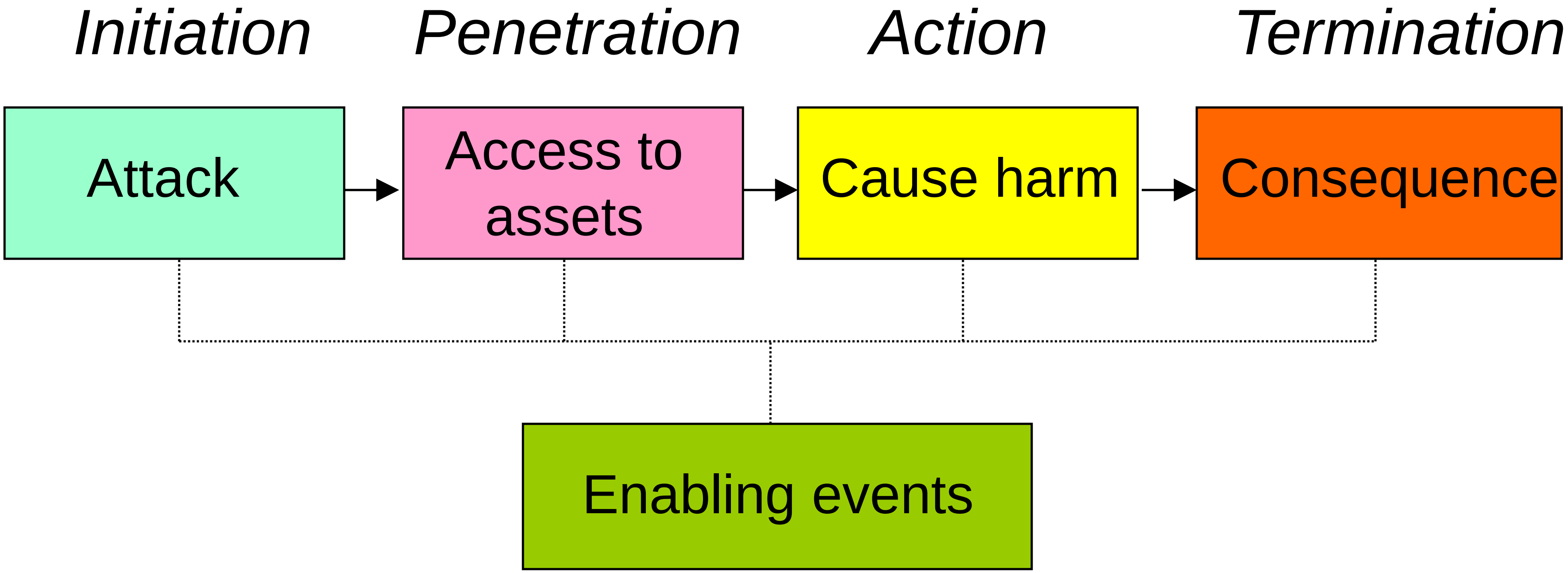
SECURITY VULNERABILITY ANALYSIS (SVA)

"Minds are like parachutes; they work best when open."
Lord Thomas Dewar

SECURITY VULNERABILITY ANALYSIS (SVA)

- Identifies ways in which deliberate acts could cause harm (*threat scenarios*)
  - How flaws or weaknesses expose a system to attack
- Determines protective measures that could be taken

THREAT SCENARIO



SVA METHODS

Method	Origination	Protect	Approach
Asset-based	Security professionals	Assets	Pairs assets with threats to define threat events
Scenario-based	Safety professionals	Against accidents	Develops more detailed scenario descriptions

SVA METHODS (CONTD.)

- Early SVA approaches focused on physical security
  - Cyber security was not considered explicitly
- Separate cyber SVA methods have subsequently been developed

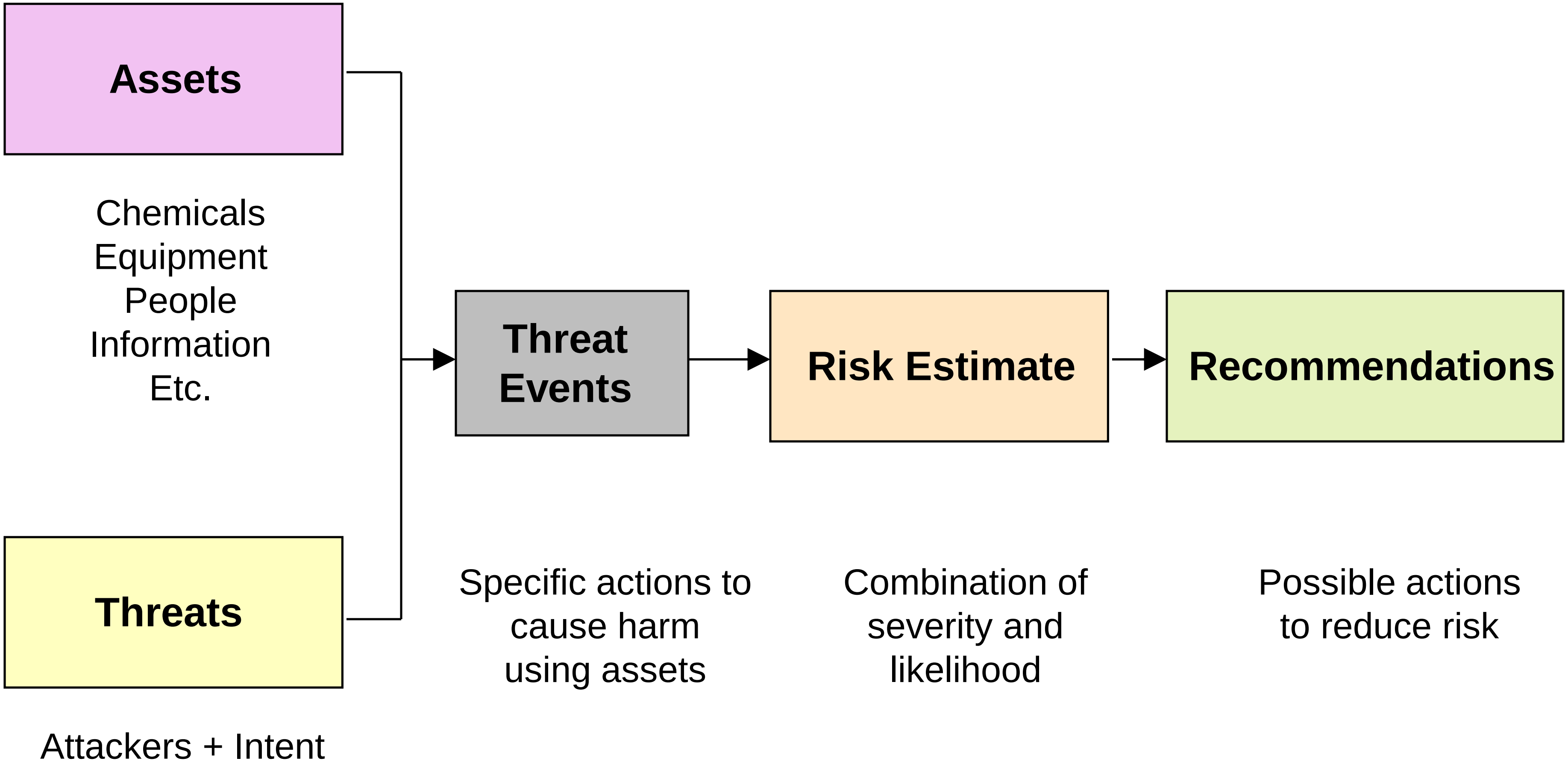
SVA METHODS (CONTD.)

- This paper focuses on how physical and cyber security can be addressed in the same study
- The SVA methods presented also:
  - Integrate asset-based and scenario-based methods into a unified approach
  - Improve on previous approaches

INTEGRATION AND IMPROVEMENT OF CYBER AND PHYSICAL SVA

> “Never mistake motion for action.”
> Ernest Hemingway

MODEL FOR SECURITY RISK ASSESSMENT



Assets

Chemicals
Equipment
People
Information
Etc.

Threats

Attackers + Intent

Threat Events

Specific actions to cause harm using assets

Risk Estimate

Combination of severity and likelihood

Recommendations

Possible actions to reduce risk

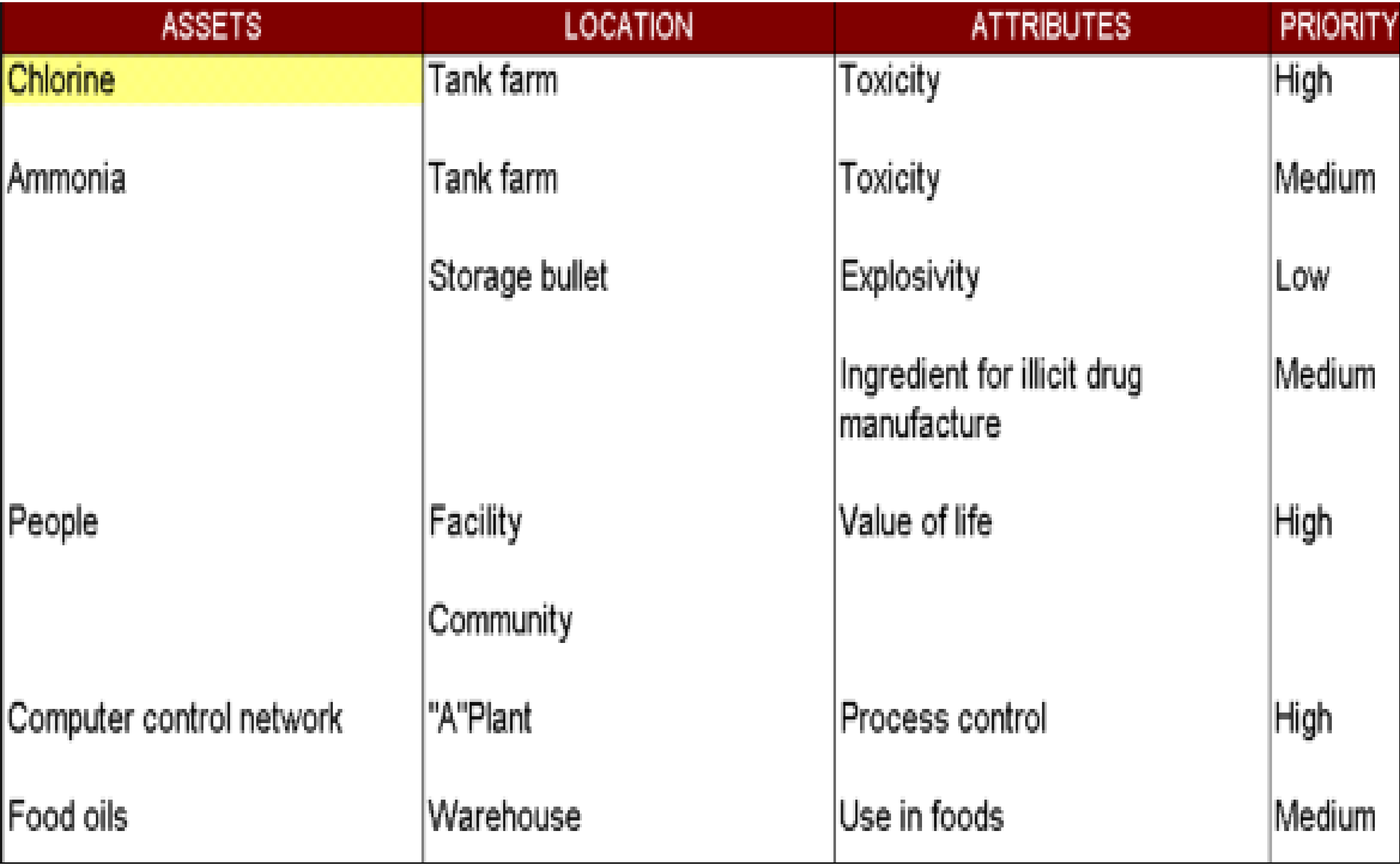
SVA STEPS

- Preparation and organization
- Target analysis
- Threat analysis
- Vulnerability analysis
- Identification of consequences
- Identification of existing countermeasures
- Estimation of risks
- Identification of recommendations
- Documentation and reporting
- Follow-up

SVA STEPS

- Preparation and organization
- ***Target analysis***
- Threat analysis
- Vulnerability analysis
- Identification of consequences
- Identification of existing countermeasures
- Estimation of risks
- Identification of recommendations
- Documentation and reporting
- Follow-up

EXAMPLE OF TARGET ANALYSIS FOR CRITICAL ASSETS

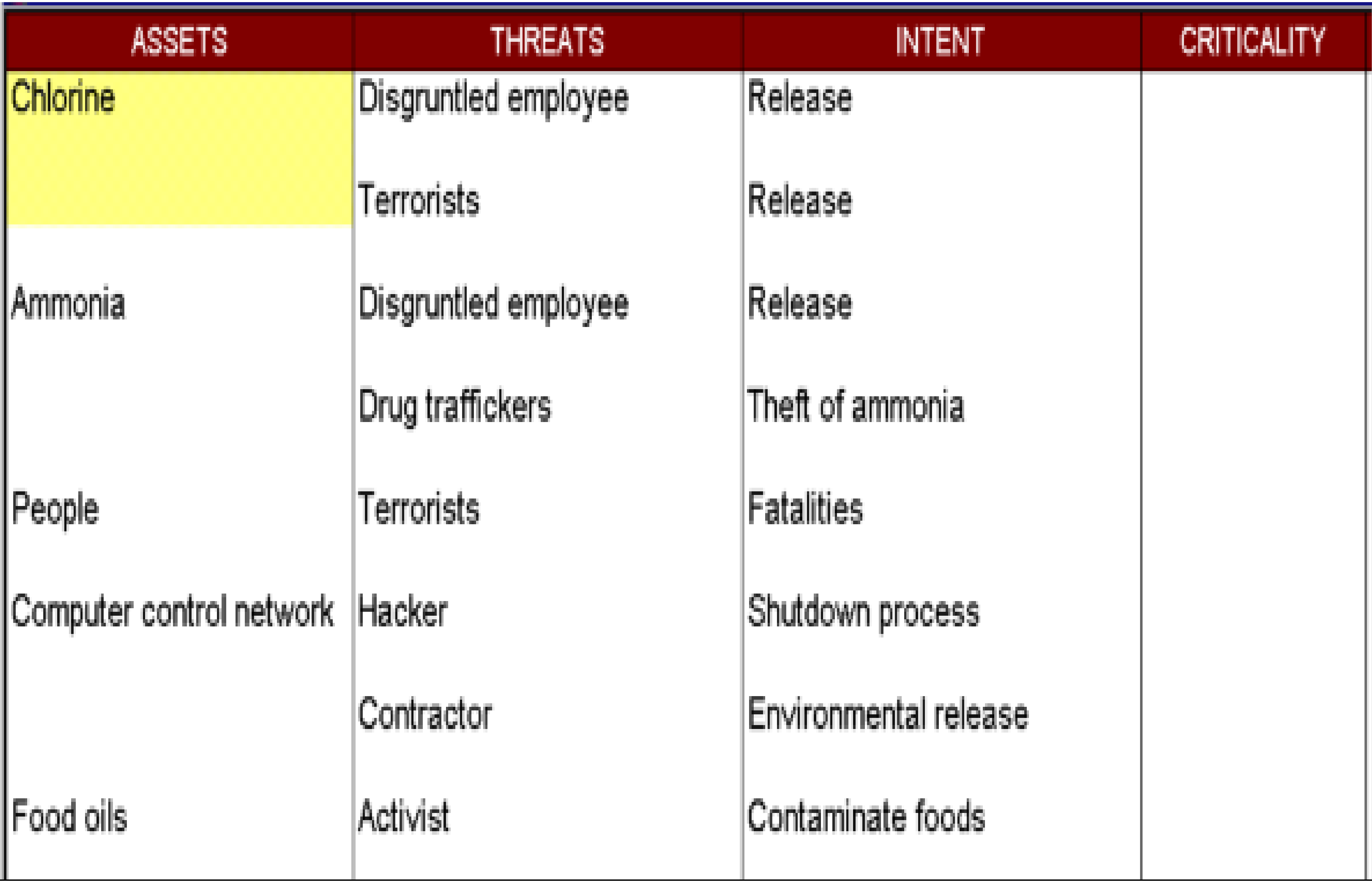


ASSETS	LOCATION	ATTRIBUTES	PRIORITY
Chlorine	Tank farm	Toxicity	High
Ammonia	Tank farm	Toxicity	Medium
	Storage bullet	Explosivity	Low
		Ingredient for illicit drug manufacture	Medium
People	Facility	Value of life	High
	Community		
Computer control network	"A"Plant	Process control	High
Food oils	Warehouse	Use in foods	Medium

SVA STEPS

- Preparation and organization
- Target analysis
- ***Threat analysis***
- Vulnerability analysis
- Identification of consequences
- Identification of existing countermeasures
- Estimation of risks
- Identification of recommendations
- Documentation and reporting
- Follow-up

EXAMPLE OF THREAT ANALYSIS

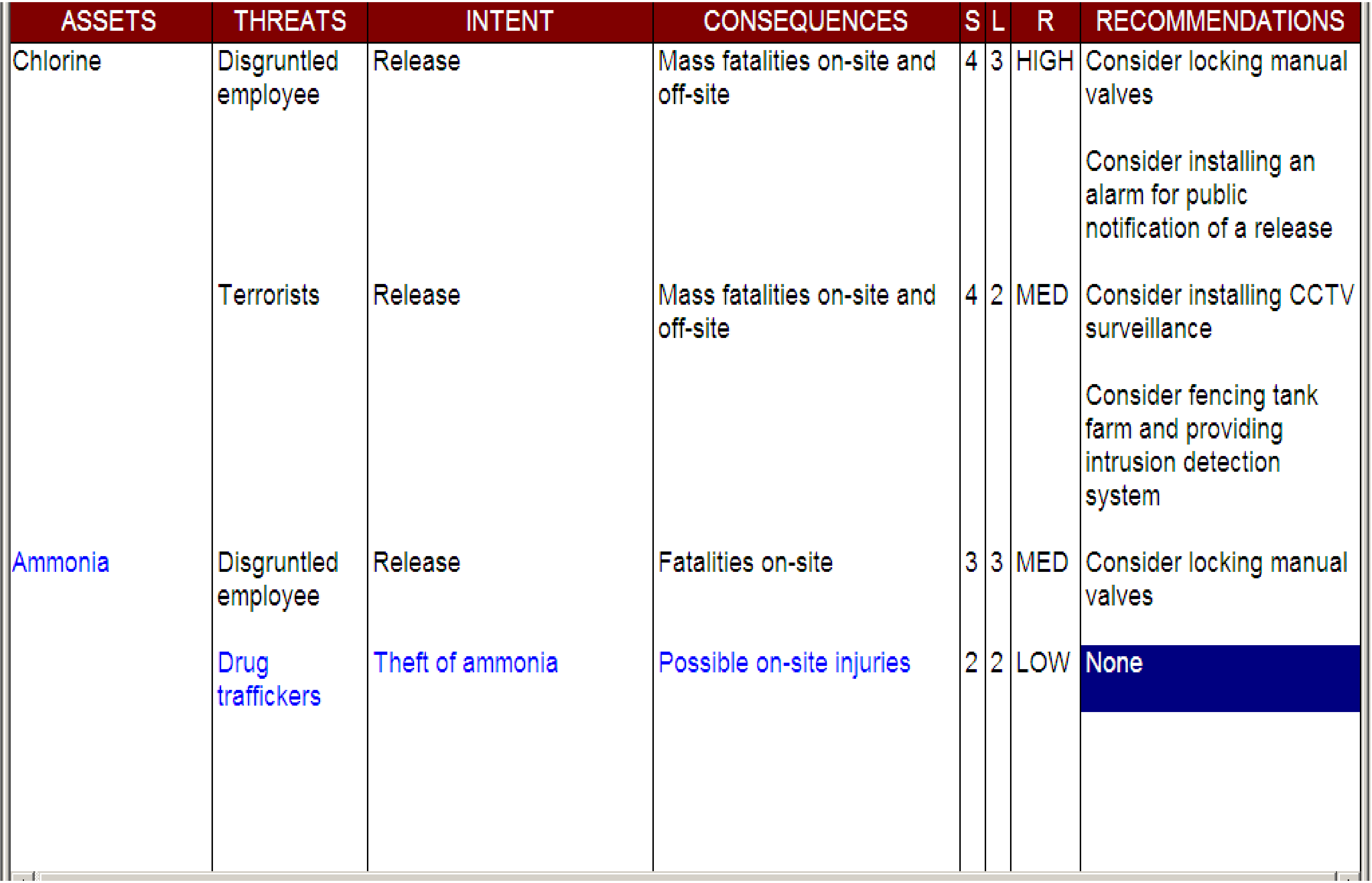


ASSETS	THREATS	INTENT	CRITICALITY
Chlorine	Disgruntled employee	Release	
	Terrorists	Release	
Ammonia	Disgruntled employee	Release	
	Drug traffickers	Theft of ammonia	
People	Terrorists	Fatalities	
Computer control network	Hacker	Shutdown process	
	Contractor	Environmental release	
Food oils	Activist	Contaminate foods	

SVA STEPS

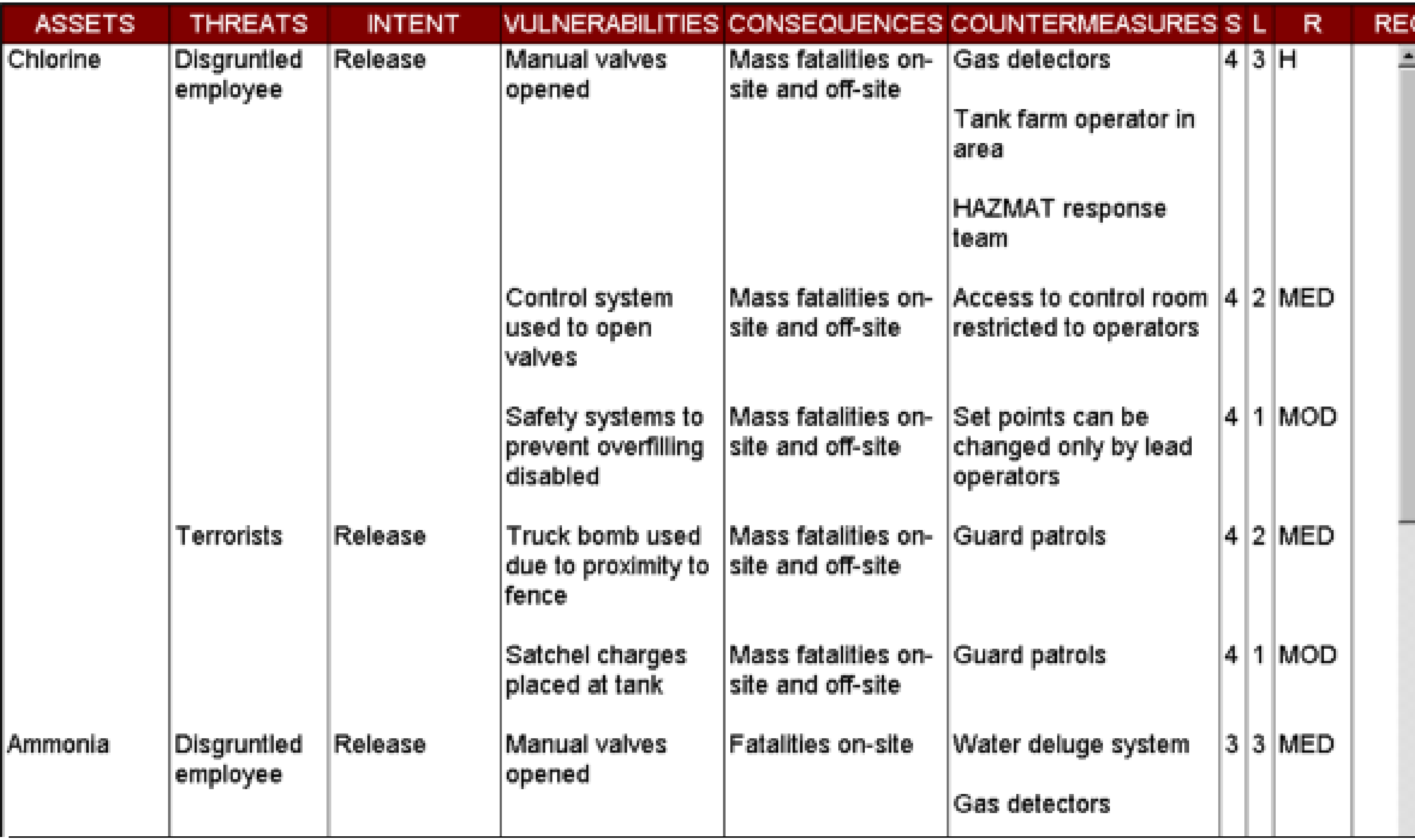
- Preparation and organization
- Target analysis
- Threat analysis
- ***Vulnerability analysis***
- ***Identification of consequences***
- ***Identification of existing countermeasures***
- ***Estimation of risks***
- ***Identification of recommendations***
- Documentation and reporting
- Follow-up

EXAMPLE OF ASSET-BASED PHYSICAL SVA



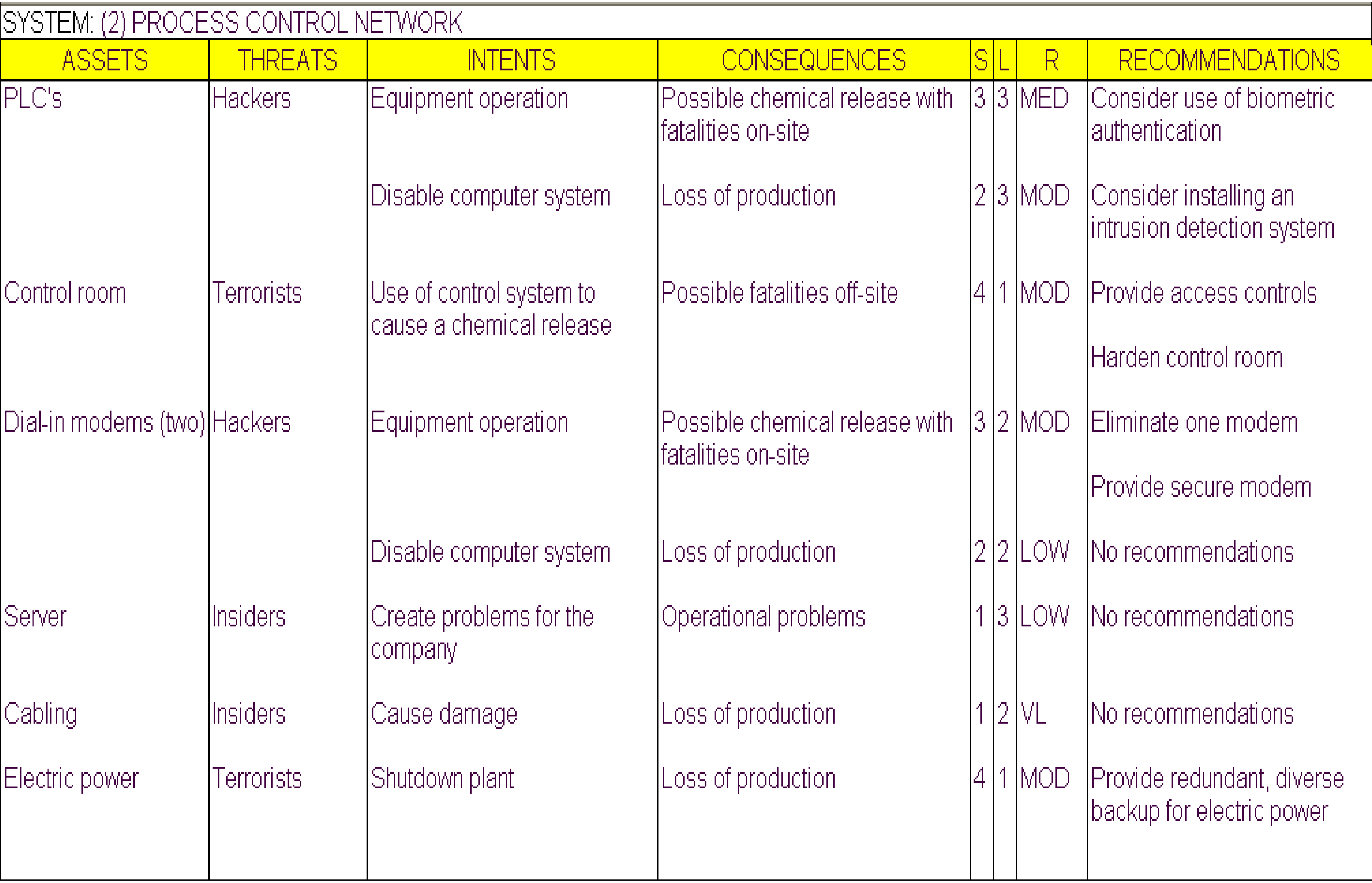
ASSETS	THREATS	INTENT	CONSEQUENCES	S	L	R	RECOMMENDATIONS
Chlorine	Disgruntled employee	Release	Mass fatalities on-site and off-site	4	3	HIGH	Consider locking manual valves Consider installing an alarm for public notification of a release
	Terrorists	Release	Mass fatalities on-site and off-site	4	2	MED	Consider installing CCTV surveillance Consider fencing tank farm and providing intrusion detection system
Ammonia	Disgruntled employee	Release	Fatalities on-site	3	3	MED	Consider locking manual valves
	Drug traffickers	Theft of ammonia	Possible on-site injuries	2	2	LOW	None

EXAMPLE OF SCENARIO-BASED PHYSICAL SVA



ASSETS	THREATS	INTENT	VULNERABILITIES	CONSEQUENCES	COUNTERMEASURES	S	L	R	REC
Chlorine	Disgruntled employee	Release	Manual valves opened	Mass fatalities on-site and off-site	Gas detectors Tank farm operator in area HAZMAT response team	4	3	H	
			Control system used to open valves	Mass fatalities on-site and off-site	Access to control room restricted to operators	4	2	MED	
			Safety systems to prevent overfilling disabled	Mass fatalities on-site and off-site	Set points can be changed only by lead operators	4	1	MOD	
	Terrorists	Release	Truck bomb used due to proximity to fence	Mass fatalities on-site and off-site	Guard patrols	4	2	MED	
			Satchel charges placed at tank	Mass fatalities on-site and off-site	Guard patrols	4	1	MOD	
Ammonia	Disgruntled employee	Release	Manual valves opened	Fatalities on-site	Water deluge system Gas detectors	3	3	MED	

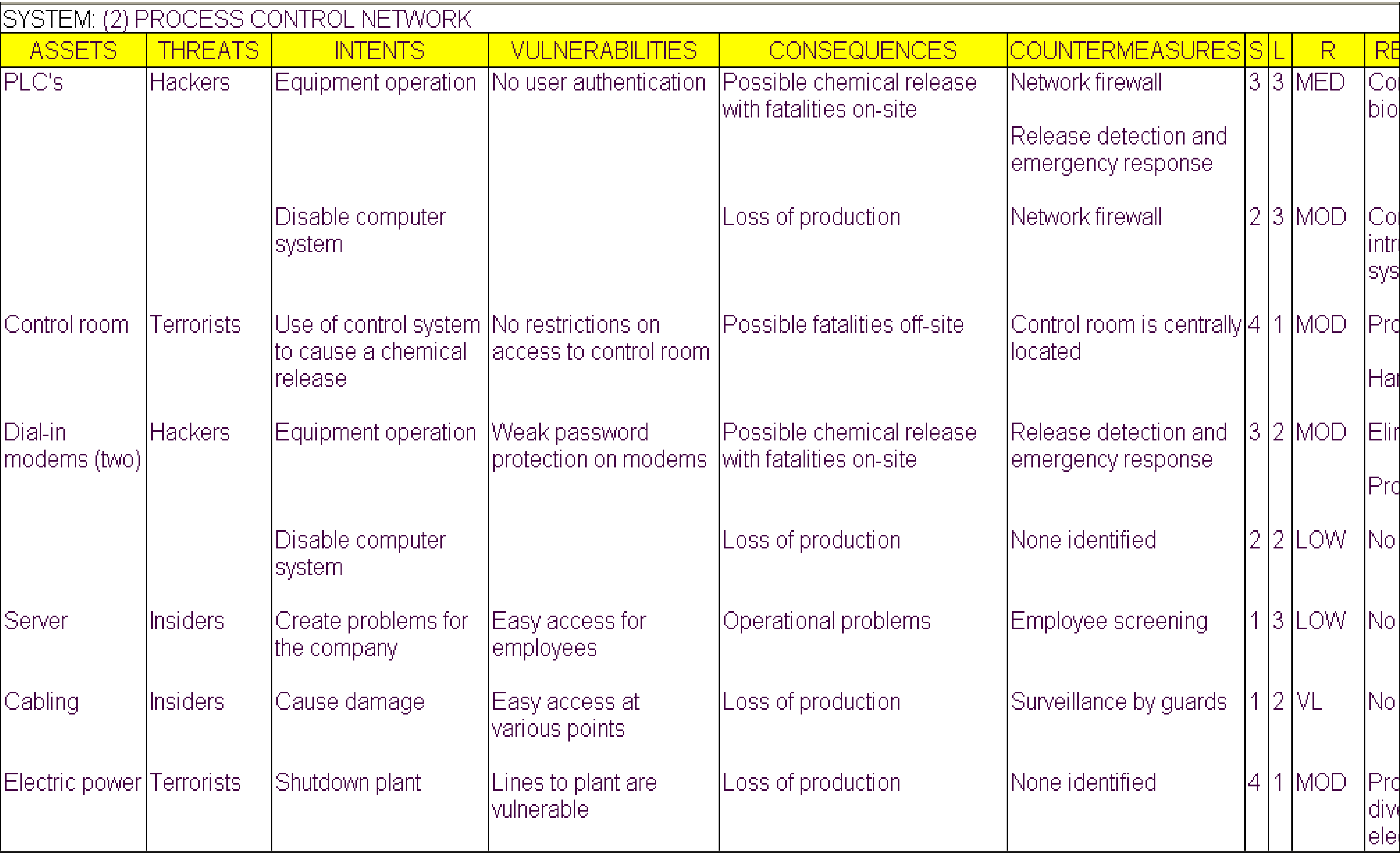
EXAMPLE OF ASSET-BASED CYBER SVA



SYSTEM: (2) PROCESS CONTROL NETWORK

ASSETS	THREATS	INTENTS	CONSEQUENCES	S	L	R	RECOMMENDATIONS
PLC's	Hackers	Equipment operation	Possible chemical release with fatalities on-site	3	3	MED	Consider use of biometric authentication
		Disable computer system	Loss of production	2	3	MOD	Consider installing an intrusion detection system
Control room	Terrorists	Use of control system to cause a chemical release	Possible fatalities off-site	4	1	MOD	Provide access controls Harden control room
Dial-in modems (two)	Hackers	Equipment operation	Possible chemical release with fatalities on-site	3	2	MOD	Eliminate one modem Provide secure modem
		Disable computer system	Loss of production	2	2	LOW	No recommendations
Server	Insiders	Create problems for the company	Operational problems	1	3	LOW	No recommendations
Cabling	Insiders	Cause damage	Loss of production	1	2	VL	No recommendations
Electric power	Terrorists	Shutdown plant	Loss of production	4	1	MOD	Provide redundant, diverse backup for electric power

EXAMPLE OF SCENARIO-BASED CYBER SVA



SYSTEM: (2) PROCESS CONTROL NETWORK

ASSETS	THREATS	INTENTS	VULNERABILITIES	CONSEQUENCES	COUNTERMEASURES	S	L	R	RE
PLC's	Hackers	Equipment operation	No user authentication	Possible chemical release with fatalities on-site	Network firewall Release detection and emergency response	3	3	MED	Co bio
		Disable computer system		Loss of production	Network firewall	2	3	MOD	Co intr sys
Control room	Terrorists	Use of control system to cause a chemical release	No restrictions on access to control room	Possible fatalities off-site	Control room is centrally located	4	1	MOD	Pro Har
Dial-in modems (two)	Hackers	Equipment operation	Weak password protection on modems	Possible chemical release with fatalities on-site	Release detection and emergency response	3	2	MOD	Elir Pro
		Disable computer system		Loss of production	None identified	2	2	LOW	No
Server	Insiders	Create problems for the company	Easy access for employees	Operational problems	Employee screening	1	3	LOW	No
Cabling	Insiders	Cause damage	Easy access at various points	Loss of production	Surveillance by guards	1	2	VL	No
Electric power	Terrorists	Shutdown plant	Lines to plant are vulnerable	Loss of production	None identified	4	1	MOD	Pro dive ele

LESSONS LEARNED

> "The only real mistake is the one from which we learn nothing."
>
> John Powell

ADVANTAGES OF COMBINING PHYSICAL AND CYBER SVA

- Economies in preparation and organization of studies
- Overlap in the team members required
- Physical attacks apply to both plant equipment and computer systems
- SVA process is similar for physical and cyber security

ADVANTAGES OFFERED BY IMPROVED SVA METHODS

- Simpler, more direct and coherent analysis
  - Results are as comprehensive
- Analysis and documentation of results is simplified
  - Single worksheet is used
  - Target analysis, threat analysis and vulnerability analysis can also be displayed in separate worksheets

ADVANTAGES OFFERED BY IMPROVED SVA METHODS (CONTD.)

- Possible to conduct the simpler, asset-based analysis first and transition smoothly into a scenario-based analysis
  - Either for the entire facility or parts of it
  - Can also go directly to a scenario-based analysis
- SVA is easily updated for revalidation
  - Or, for change and configuration management

ADVANTAGES OFFERED BY IMPROVED SVA METHODS (CONTD.)

- Format similar to PHA
  - Benefits PHA team members who will participate in SVAs
- Structured around a classical risk analysis framework
  - Can be updated and modified easily to benefit from future technical developments

CONCLUSIONS

- Risk of malevents for process plants is real
- Must be assessed and managed for all credible threats
  - SVA is the key
- A process security management program should be implemented

FURTHER INFORMATION

- Technical papers on cyber and physical SVA and management systems:

  www.primatech.com

- Contact info:

  paulb@primatech.com