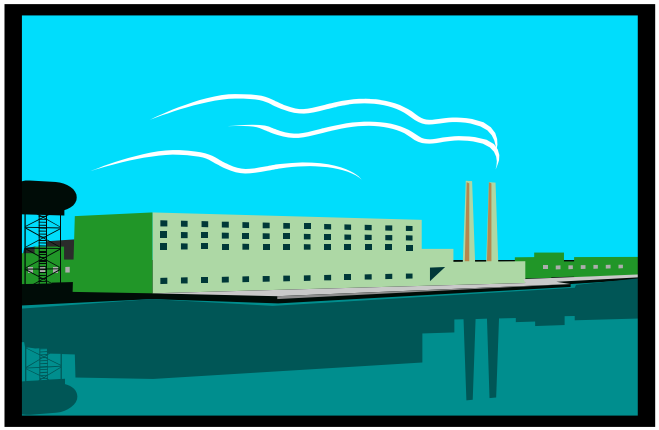
CYBER SECURITY VULNERABILITY ANALYSIS: LESSONS LEARNED FROM THE APPLICATION OF THREE METHODS

Paul Baybutt, Primatech Inc.

and Blair Moore, Occidental Inc.

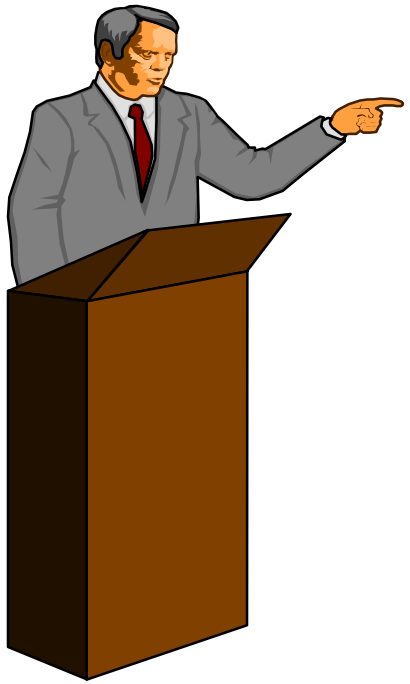
ISA Conference

October, 2003



OVERVIEW

- Meaning of cyber security
- Cyber security vulnerability analysis
- Methods used
- Lessons learned

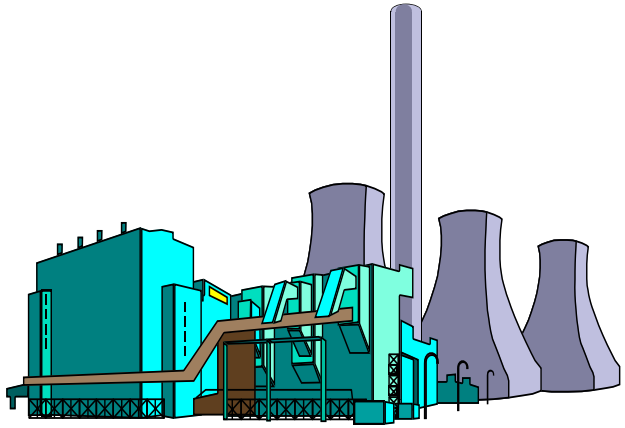


"Real knowledge is to know the extent of one's ignorance."

Confucius

CYBER SECURITY FOR MANUFACTURING AND PROCESS PLANTS

TARGETS	PURPOSE
Stored information	Obtain, corrupt, damage, destroy or prohibit access
Computer systems	Disable
Controls	Manipulate

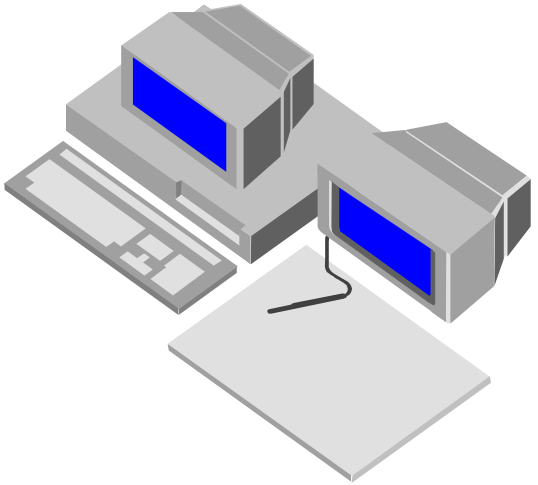


POTENTIAL CONSEQUENCES OF CYBER ATTACKS

- Interference with production
- Process shutdown
- Process / equipment / product damage
- Diversion or theft of materials
- Contamination of products
- Spoiled products
- Release of hazardous materials
- Runaway reaction

COMPUTER SYSTEMS TO CONSIDER

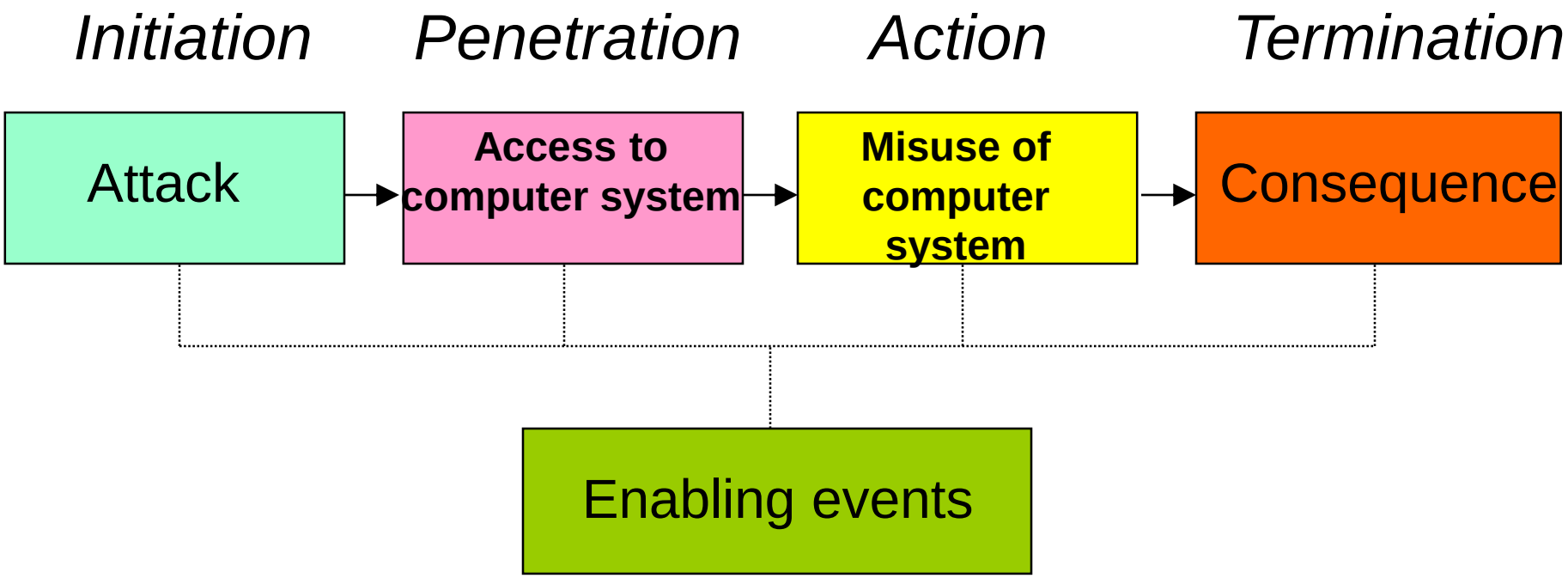
- Manufacturing and process control
- Safety systems operation
- Information storage
- Facility access
- Networks



CYBER SECURITY VULNERABILITY ANALYSIS (CSVA)

- Identify threats to assets from attackers
- Evaluate vulnerabilities
- Consider existing countermeasures
- Estimate risks
- Determine need for additional countermeasures

CYBER THREAT SCENARIO



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

John Powell

CSVA METHODS USED

- Scenario-based
- Asset-based
- Sneak path

"Knowing is not enough; we must apply. Willing is not enough; we must do."

Johann von Goethe

ELEMENTS OF CYBER THREAT SCENARIOS

- Sources/assailants/attackers
- Assets/targets
- Intents
- Vulnerabilities/paths
- Countermeasures/barriers
- Consequences/events

SCENARIO-BASED

- Couple assailants and intent to focus on *threats*
- Identify vulnerabilities to threats
  - Best kept at high level
  - Similar for similar assailants
- Determine consequences
  - Similar for all vulnerabilities to a particular threat
- Identify existing safeguards/countermeasures
- Perform risk ranking
- Specify recommendations for new countermeasures

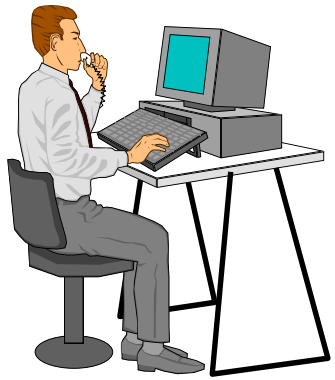
CSVA-SB WORKSHEET

SYSTEM: (1) PROCESS CONTROL SYSTEM

THREATS	VULNERABILITIES	CONSEQUENCES	SAFEGUARDS	S	L	R	RECOMMENDATIONS	BY
Manipulation of process control system by disgruntled employee to cause a release of hazardous material	1. Dialup modem in process control system allows remote access	1.1. Possible employee fatalities	1.1.1. Dike 1.1.2. Gas detectors	3	3	B	1.1.1. Consider eliminating dialup modems	IT
		1.2. Possible offsite fatalities	1.2.1. Same as 1.1.1 and 1.1.2	4	3	C		
	2. Internet connection of PC connected to control system allows remote access	2.1. Possible employee fatalities	2.1.1. Same as 1.1.1 and 1.1.2	3	3	B	2.1.1. Consider restricting employee remote access to control system	OPS
							2.1.2. Consider automatic notification of operators when control computers are remotely accessed	IT

ASSET-BASED

- Focus on assets
- Identify threats to assets
  - Combination of assailants and intent
- Determine consequences
- Develop recommendations
  - Considering vulnerabilities and existing countermeasures



CSVA-AB WORKSHEET

CSVA-Pasadena: System 1

SYSTEM: (1) PLANT COMPUTER SYSTEMS

ASSETS	THREATS	INTENT	CONSEQUENCES	S	L	R	RECOMMENDATIONS	E
PLC's	Hackers	Equipment operation	Possible chemical release with on-site fatalities	3	3	B	Consider use of biometric authentication	
		Disable computer system	Loss of production	2	3	B	Consider installing an intrusion detection system	
Control room	Terrorists	Use of control system to cause a chemical release	Possible fatalities off-site	4	1	B	Provide access controls Harden control room	
Dial-up modem	Hackers	Equipment operation	Possible chemical release with on-site fatalities	3	2	B	Provide secure modem	
		Disable computer system	Loss of production	2	2	A	No recommendations	
Server	Insiders	Create problems for the company	Operational problems	1	3	A	No recommendations	

SNEAK PATH

- Consider assailants (sources) and assets (targets)
- Identify ways they can be combined through vulnerabilities (paths)
- Identify countermeasures (barriers)
- Determine consequences (events)
- Develop recommendations

CSVA-SP WORKSHEET

SYSTEM: (1) PLANT COMPUTER SYSTEMS

SOURCES	TARGETS	PATHS	BARRIERS	EVENTS	S	L	R	RECOMMENDATIONS
Hacker	Reactor temperature control set points	Internet connection directly to site LAN	LAN firewall	Runaway reaction	4	1	B	Consider intrusion detection system
		Dialup modem on PC connected to PCN	Password	Runaway reaction	4	2	B	Consider removal of PC
		Contractor network and use of dial-up modem connection to LAN	PCN firewall	Runaway reaction	4	1	B	Consider use of secure modem
Disgruntled employee	Tank farm control valves	HMIs	Fellow operators Alarms	Spill to dike	2	2	A	None
		Desktop PC		Spill to dike	2	3	B	Consider removal of PC
		EWS in engineer's		Spill to dike	2	2	A	None

DIFFERENCES BETWEEN METHODS

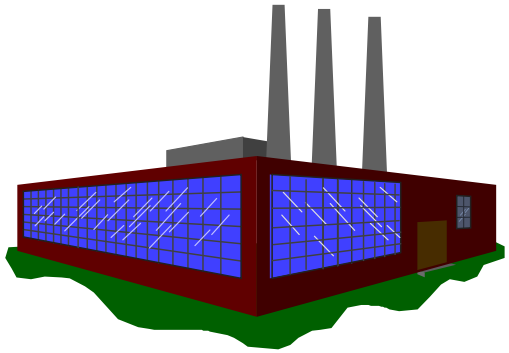
- Anchor point used
- Aspects of scenario included
  - Can be varied
- Level of detail
  - Can be varied

LESSONS LEARNED

- Plant and IT personnel have different perspectives
  - Facilitate communication
  - Reconcile different agendas
- Team members from physical SVA or PHA can help explain the process to new team members
- Regardless of the techniques used, complete an entire scenario first before completing columns vertically
  - Ensures team understands the process

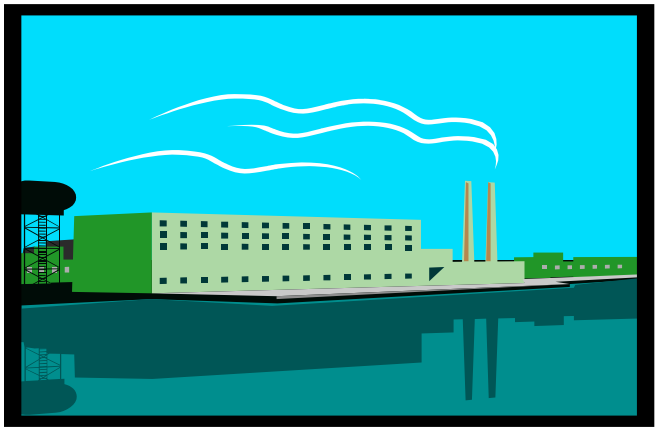
LESSONS LEARNED (CONTD.)

- Limit sessions to half days and take the time needed
- Ensure risk ranking scheme provides sufficient discrimination between scenarios
- All three methods require the same size team
- Difficult to analyze plant systems separately
  - corporate computer systems need to be addressed



CONCLUSIONS

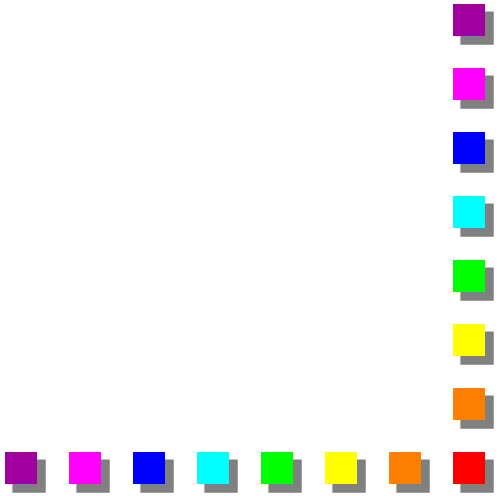
- Scenario-based method appeals to process plant personnel
- Asset-based method appeals to IT personnel
- All three methods produce essentially equivalent results



CONTACT INFORMATION

paulb@primatech.com

blairmoore@cidx.com



FURTHER INFORMATION – TECHNICAL PAPERS

A. Screening Facilities For Cyber Security Risk Analysis
B. An Asset-based Approach For Cyber Security Vulnerability Analysis
C. Cyber Security Vulnerability Analysis: A Scenario-based Approach
D. Sneak Path Analysis Applied To Industrial Cyber Security
E. Audit Protocols For Industrial Cyber Security
F. Cyber Security Risk Analysis For Process Control Systems - Rings Of Protection Analysis (ROPA)
G. Industrial Cyber Security Management Programs
H. Making Sense Of Cyber Security