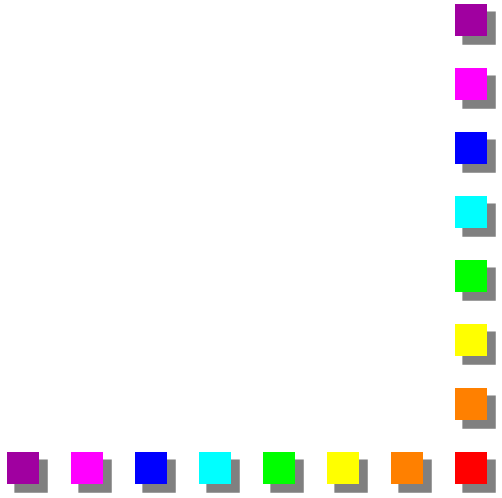
CYBER SECURITY VULNERABILITY ANALYSIS FOR THE CHEMICAL SECTOR

Blair Moore,
Cybersecurity Director, Chemical Industry Data Exchange
and
Paul Baybutt
President, Primatech Inc.

ACC Security Summit
Philadelphia, PA
June 28, 2004

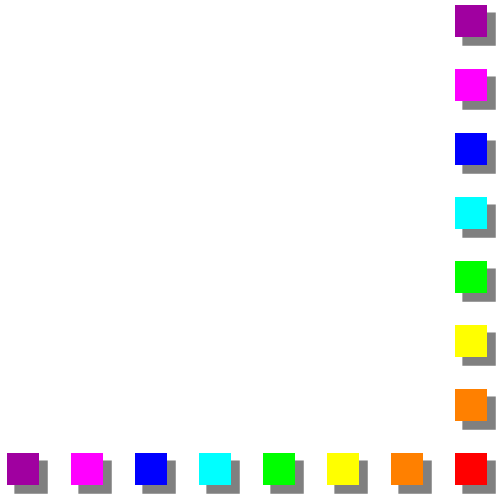


OUTLINE

- What is cyber security?
- Why is cyber security an issue?
- What can be done about cyber security?
- How should I proceed?

> “Real knowledge is to know the extent of one's ignorance.” Confucius

What is cyber security?

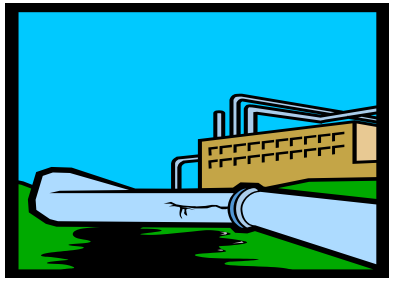


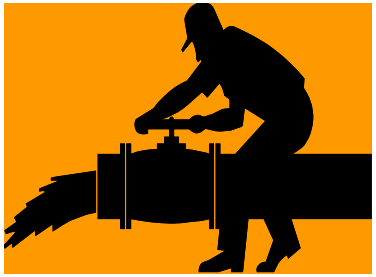
EXTRAORDINARY EVENTS

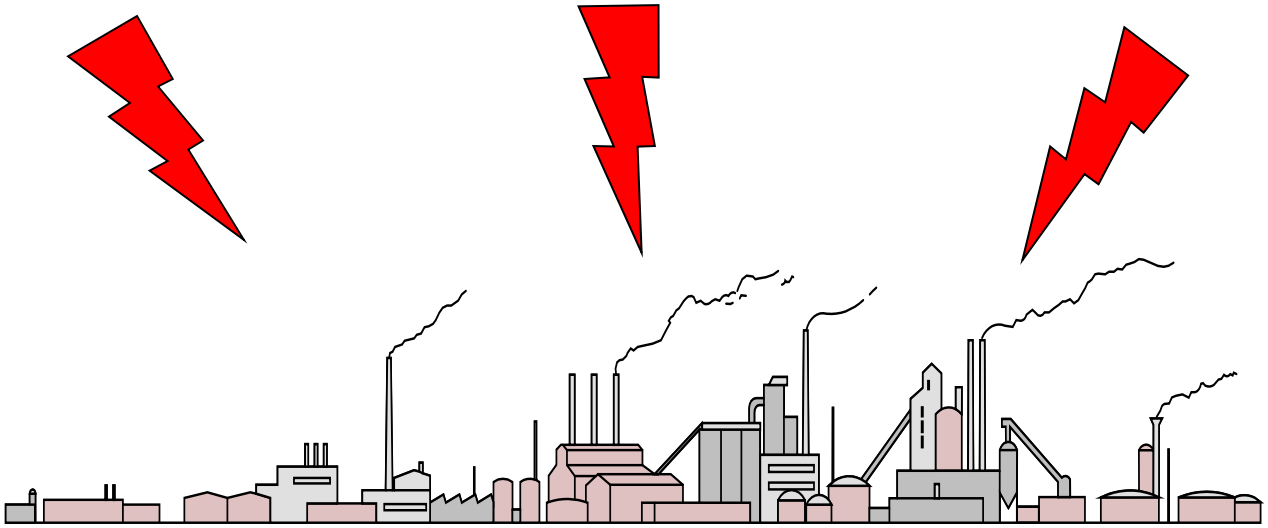
Accidents

Natural Events

Deliberate Acts







TYPES OF THREATS

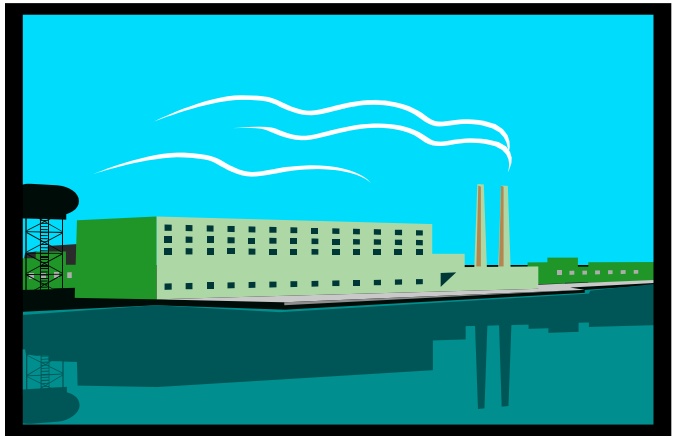
- Physical
- Cyber

CYBER SECURITY – INFORMATION TECHNOLOGY

- Historically, computers attacked for the information stored in them
- IT cyber security focused on the security of information
  - Cannot be read, compromised or stolen
  - Established discipline for commercial and business computer systems

CYBER SECURITY - MANUFACTURING AND PROCESS PLANTS

- Needs to be defined more broadly
  - Include a range of malicious acts that could be perpetrated through access to a computer system

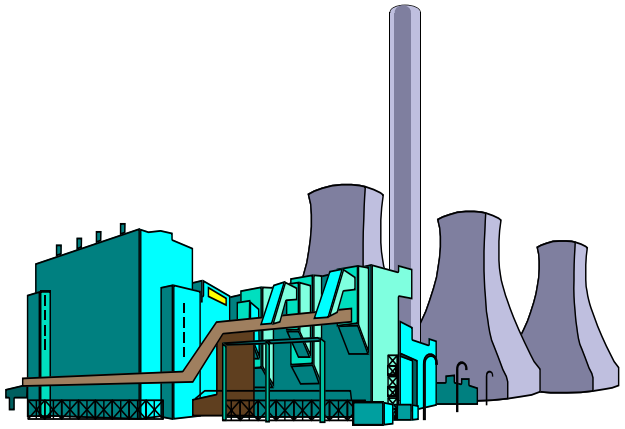


POTENTIAL CONSEQUENCES OF CYBER ATTACKS

- 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

CYBER SECURITY FOR MANUFACTURING AND PROCESS PLANTS

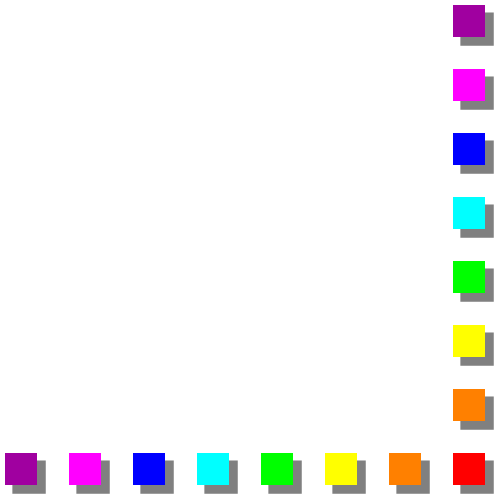
- Protection of manufacturing and process plant computer systems from:
  - Cyber or physical attack by adversaries who wish to disable or manipulate them to cause harm
  - Access by adversaries who want to obtain, corrupt, damage, destroy or prohibit access to valuable information



SCOPE OF CYBER SECURITY

- All types of computer systems
  - Manufacturing and process control
  - Safety systems operation
  - Utility operation
  - Facility access
  - Business systems
  - Communications systems
  - Etc.
- All parts of the value chain
  - Manufacturing
  - Transportation
  - Distribution
  - Etc.

Why is cyber security an issue?



INFORMATION TECHNOLOGY CYBER SECURITY

- Became an issue when the computers on which information is stored became part of networks
  - Particularly ones connected to the Internet

INDUSTRIAL CYBER SECURITY

- Historically, process control systems have been kept separate from business computer systems
  - Increasingly they are being connected through networks
  - DCS, PLC, SCADA
- This exposes control systems to penetration

HACKER ATTACK

- Slammer worm was released in January 2003
- Caused havoc with various systems, e.g.
  - 911 call center in Seattle taken offline
  - Delayed and canceled airline flights
  - Bank of America ATMs disabled

J. Moore, Check Your Locks, ISA News and Views, July, 2003.

HACKER ATTACK (CONTD.)

- Also, industrial impacts occurred:
  - Utility's critical SCADA network was downed when Slammer moved from a corporate network to the control center LAN
  - Another utility lost its Frame Relay network used for communications
  - Some petrochemical plants lost HMIs and data historians

HACKER ATTACK (CONTD.)

- Slammer penetrated a computer network at Ohio's Davis-Besse nuclear power plant
- Disabled a safety monitoring system for nearly five hours
  - Despite a belief by plant personnel that the network was protected by a firewall
- Event occurred due to an unprotected interconnection between plant and corporate networks

HACKER ATTACK (CONTD.)

- These were the effects of the release of one *unintelligent* piece of malicious software
- No specific facility was targeted

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

SABOTAGE OF A WASTE-TREATMENT PLANT

- Waste treatment system in Queensland, Australia
- Attacked through a wireless network access point
- Millions of gallons of raw sewage were diverted to local parks and rivers
  - by an individual who worked for the company that installed the system
- Individual responsible was angry over a rejected job application
- Found guilty and sent to prison for 2 years

T. Smith, "Hacker Jailed for Revenge Sewage Attacks", UK Register, 10/31/01

TERRORISTS

- Evidence exists that al Qaeda terrorists have investigated the availability of software and programming information
  - For systems that run US power, water, transport and communications

Al Qaeda Studies Cyberattack Systems, Infotech, September, 2002.

THREATS ARE REAL

- Presently, it is likely there are more people trying to break into computer systems than trying to prevent intrusions
- Sophisticated hacking tools exist
- Insiders may manipulate control systems

POTENTIAL ATTACKERS

- Hackers
- Disgruntled employees or other insiders
- Professional thieves
- Terrorists
- Competitors
- Adversary nations

Note: Data on cyber attacks indicate that about 70% of actual attacks are made by insiders

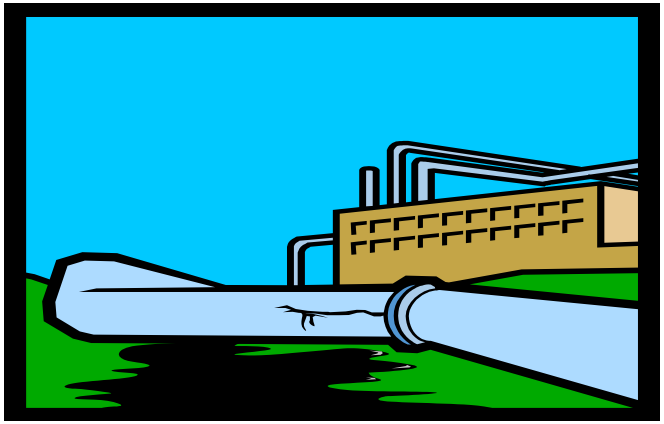
CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2001

VULNERABILITIES EXIST

- Control systems are 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

VULNERABILITIES EXIST (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



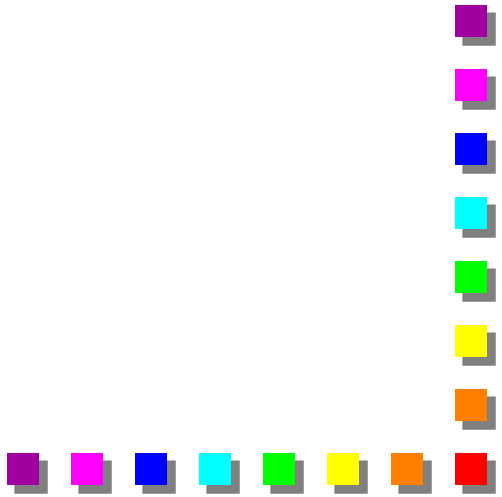
TYPES OF ATTACK

- Attackers may have specific objectives to cause harm
- Attackers may simply want to penetrate a system
  - Harm may then be caused deliberately or inadvertently as they explore the system

TYPES OF ATTACK (CONTD.)

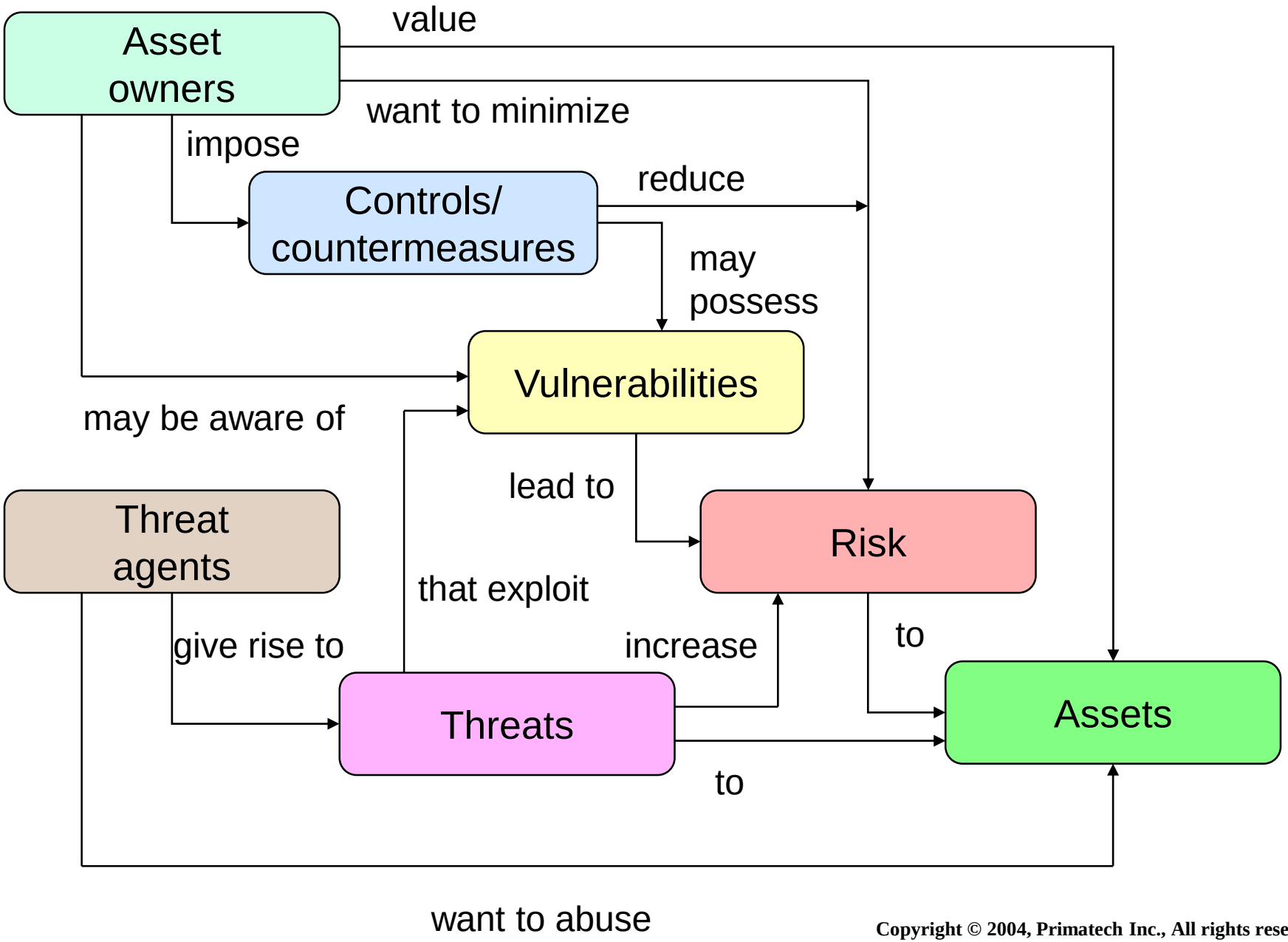
- Theft, corruption, damage or destruction of information
- Denial of service
- Manipulation, e.g.
  - Opening/closing valves
  - Disabling alarms
  - Changing set points for such process parameters as pressure, temperature, and level
  - Overriding alarm and trip settings
- Loss of control and shutdown

What can I do about cyber security?



"As long as we keep the computer turned off, we'll be completely hacker proof."

SECURITY CONCEPTS AND RELATIONSHIPS

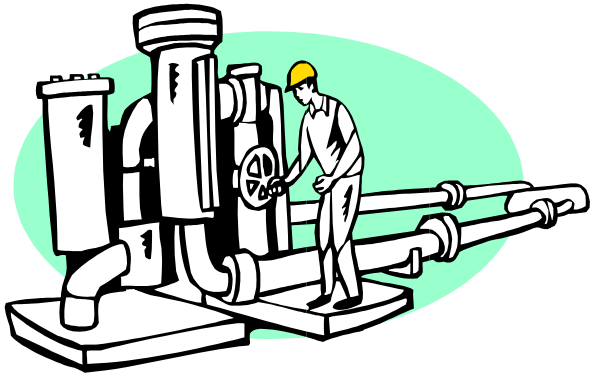


CYBER SECURITY ASSESSMENT METHODS

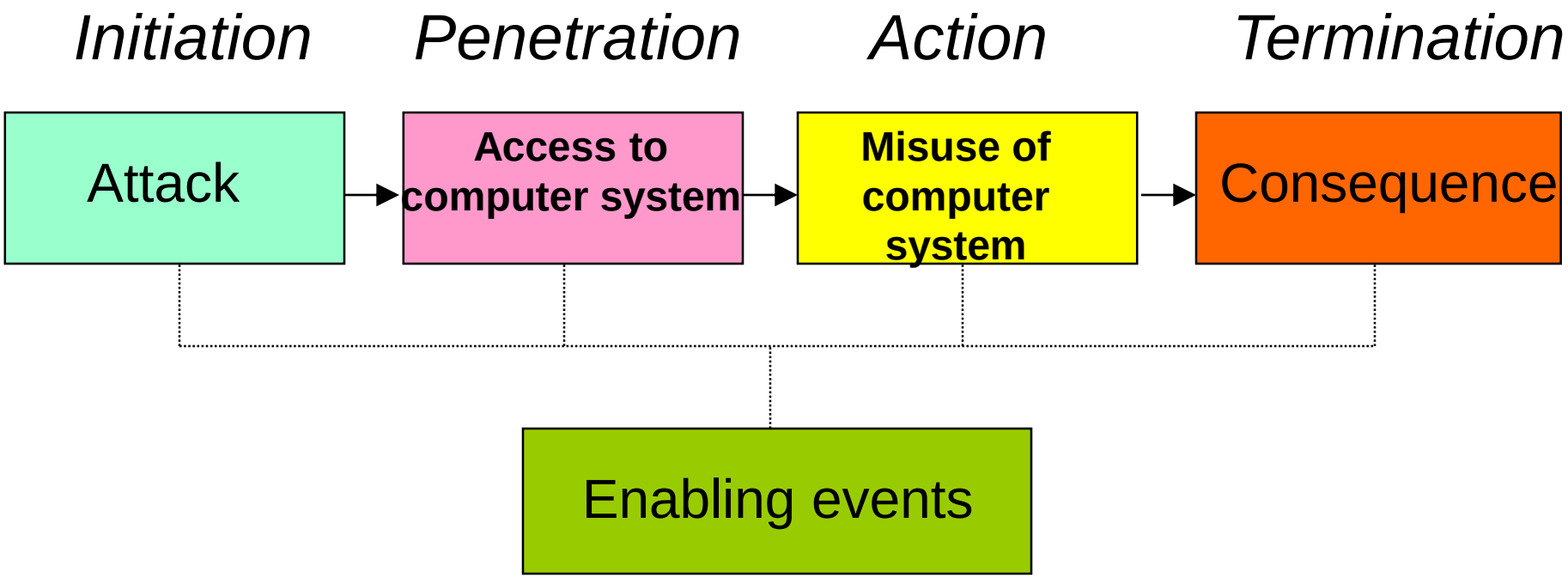
- Risk assessment
  - Qualitative
  - Quantitative
- Vulnerability analysis
  - Asset-based
  - Scenario-based
  - Sneak path
- Reviews and audits

SECURITY VULNERABILITY ANALYSIS (SVA)

- Identify ways in which deliberate acts could cause harm (threat scenarios)
- Determine protective measures that could be taken



CYBER THREAT SCENARIO



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

John Powell

STEPS IN CSVA-SB

1) Divide computer system/process/facility into systems/subsystems
2) List credible threats within each system/subsystem
3) Identify vulnerabilities within each system/subsystem
4) List worst possible consequences
5) List existing security measures and safeguards
6) Risk rank scenarios (optional)
7) Identify any recommendations

STEP 1 – DIVIDE INTO SYSTEMS/SUBSYSTEMS

- Subdivision helps
  - Focus the analysis
  - Provides a suitable level of detail
- Use a global system:
  - Account for malevents that arise within multiple systems/subsystems and/or affect the entire facility/process

CSVA WORKSHEET

SYSTEM: (1) PROCESS CONTROL SYSTEM

THREATS	VULNERABILITIES	CONSEQUENCES	SAFEGUARDS	S	L	R	RECOMMENDATIONS	BY

STEP 2 - THREATS

- Identify attackers and their actions

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

CSVA 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								
Shutdown of process control system by hacker								

STEP 3 - VULNERABILITIES

- Brainstorm ways in which specific threats could be realized
  - Identify how the computer system can be penetrated and what malicious actions can be taken once access has been gained

"You can tell whether a man is clever by his answers. You can tell whether a man is wise by his questions." Naguib Mahfouz

CSVA 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 2. Internet connection of PC connected to control system allows remote access 3. Engineers can upload software to process control computers possibly containing backdoors							
Shutdown of process control								

STEP 4 - CONSEQUENCES

- Conservatively, assume the worst consequences
- Possible consequences include:
  - Employee and public fatalities, injuries and health effects
  - Environmental impacts
  - Financial impacts
  - Damage to the economy and the infrastructure of society
  - Loss of public confidence

CSVA 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						
		1.2. Possible offsite fatalities						
	2. Internet connection of PC connected to control system allows remote access	2.1. Possible employee fatalities						
		2.2. Possible offsite fatalities						
	3. Engineers can upload software to process control computers possibly containing backdoors	3.1. Possible employee fatalities						
		3.2. Possible offsite fatalities						

STEP 5 – SECURITY MEASURES AND SAFEGUARDS

- List applicable security measures and safeguards
- May address prevention, detection, control, and mitigation of cyber attacks

CSVA 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					
		1.2. Possible offsite fatalities	1.2.1. Same as 1.1.1 and 1.1.2					
	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					
		2.2. Possible offsite fatalities	2.2.1. Same as 1.1.1 and 1.1.2					
	3. Engineers can upload software to process control computers possibly containing backdoors	3.1. Possible employee fatalities	3.1.1. Same as 1.1.1 and 1.1.2					
		3.2. Possible offsite fatalities	3.2.1. Same as 1.1.1 and 1.1.2					

STEP 6 – RISK RANKING

- Optionally estimate the severity and likelihood of each threat scenario
- Risk levels can be used to:
  - Determine if recommendations for risk reduction are needed
  - Prioritize recommendations

CSVA 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	3	3	B		
			1.1.2. Gas detectors					
		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		
		2.2. Possible offsite fatalities	2.2.1. Same as 1.1.1 and 1.1.2	4	3	C		
	3. Engineers can upload software to process control computers possibly containing backdoors	3.1. Possible employee fatalities	3.1.1. Same as 1.1.1 and 1.1.2	3	2	B		
		3.2. Possible offsite fatalities	3.2.1. Same as 1.1.1 and 1.1.2	4	2	B		

STEP 7 - RECOMMENDATIONS

- Identify any recommendations for additional and/or strengthened countermeasures
  - Based on the nature of the threat, vulnerabilities, possible consequences and existing security measures and safeguards

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

Johann von Goethe

CSVA WORKSHEET

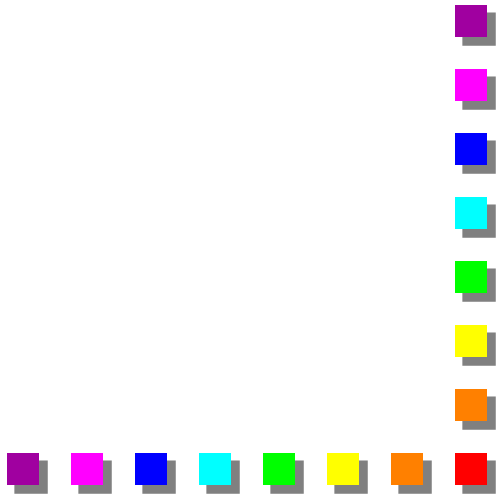
SYSTEM: (1) PROCESS CONTROL SYSTEM

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	3	3	B	1.1.1. Consider eliminating dialup modems	IT
			1.1.2. Gas detectors					
		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

CSVA LESSONS LEARNED

- Define systems as networks
- Ensure both IT and control systems personnel participate
- Plant and IT personnel have different perspectives
  - Facilitate communication
  - Reconcile different agendas
- Team members for physical SVA or PHA can help explain the process to new team members

How should I proceed?



PLAN OF ACTION

- Add cyber security to your company's values
- Ensure someone takes ownership of cyber security and hold them accountable
- Immediately conduct a review or audit of your current cyber security measures
  - Implement obvious fixes

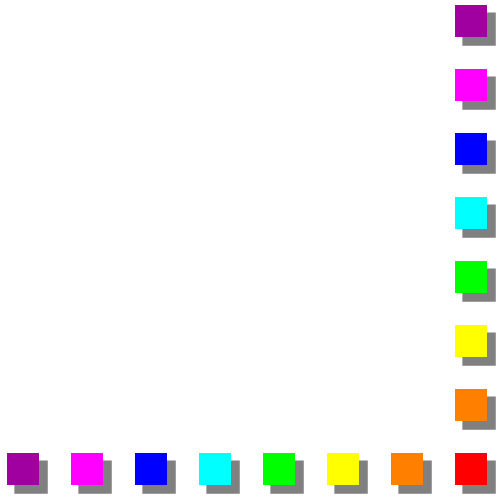
"Never mistake motion for action. "Ernest Hemingway

PLAN OF ACTION (CONTD.)

- Follow up with a cyber security vulnerability analysis
  - Provides a more complete identification of your vulnerabilities and recommendations on further corrective actions
- Implement a cyber security management system
  - Ideally by integrating it into your existing management systems for safety, quality, etc.

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

CONCLUSIONS



FURTHER INFORMATION – TECHNICAL PAPERS

A. Making Sense Of Cyber Security
B. Screening Facilities For Cyber Security Risk Analysis
C. An Asset-based Approach For Cyber Security Vulnerability Analysis
D. Cyber Security Vulnerability Analysis: A Scenario-based Approach
E. Sneak Path Analysis Applied To Industrial Cyber Security
F. Cyber Security for the Manufacturing Value Chain and IT Systems
G. Audit Protocols for Industrial Cyber Security
H. Cyber Security Risk Analysis For Process Control Systems - Rings Of Protection Analysis (ROPA)
I. Cyber Security Management Systems
J. Human Factors in Cyber Security