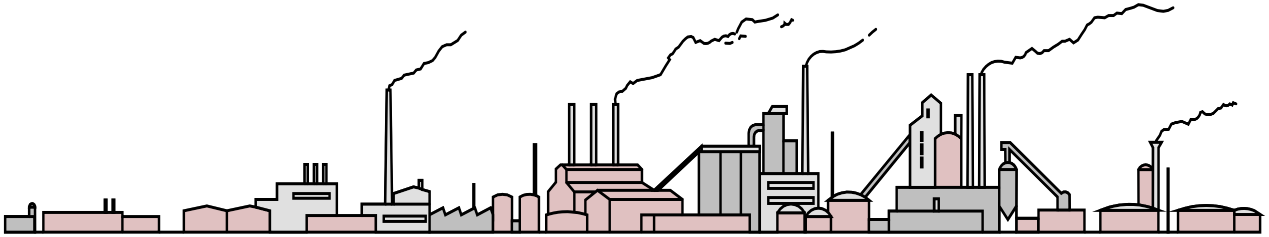
LESSONS LEARNED IN CONDUCTING CYBER SECURITY VULNERABILITY ANALYSIS

by Paul Baybutt, Primatech Inc.

Presented at the ISA Expo Technical Conference on Manufacturing & Control Systems Security, Chicago, October 25, 2005

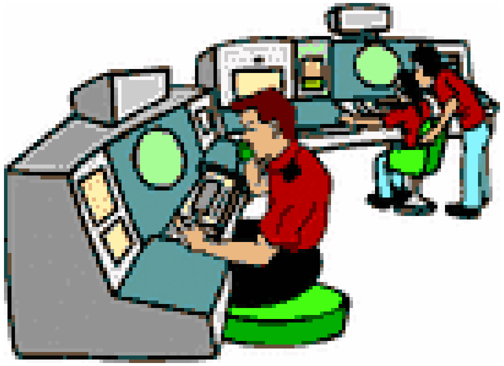
paulb@primatech.com

www.primatech.com



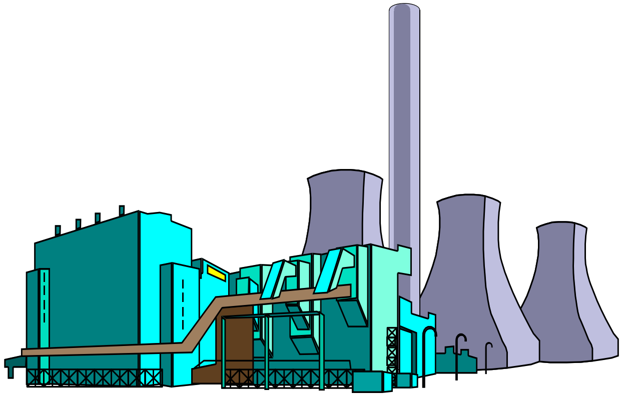
OVERVIEW

- Cyber security and the protection of computer systems
- Managing cyber security and risk assessment
- Cyber security vulnerability analysis (SVA)
- Lessons learned

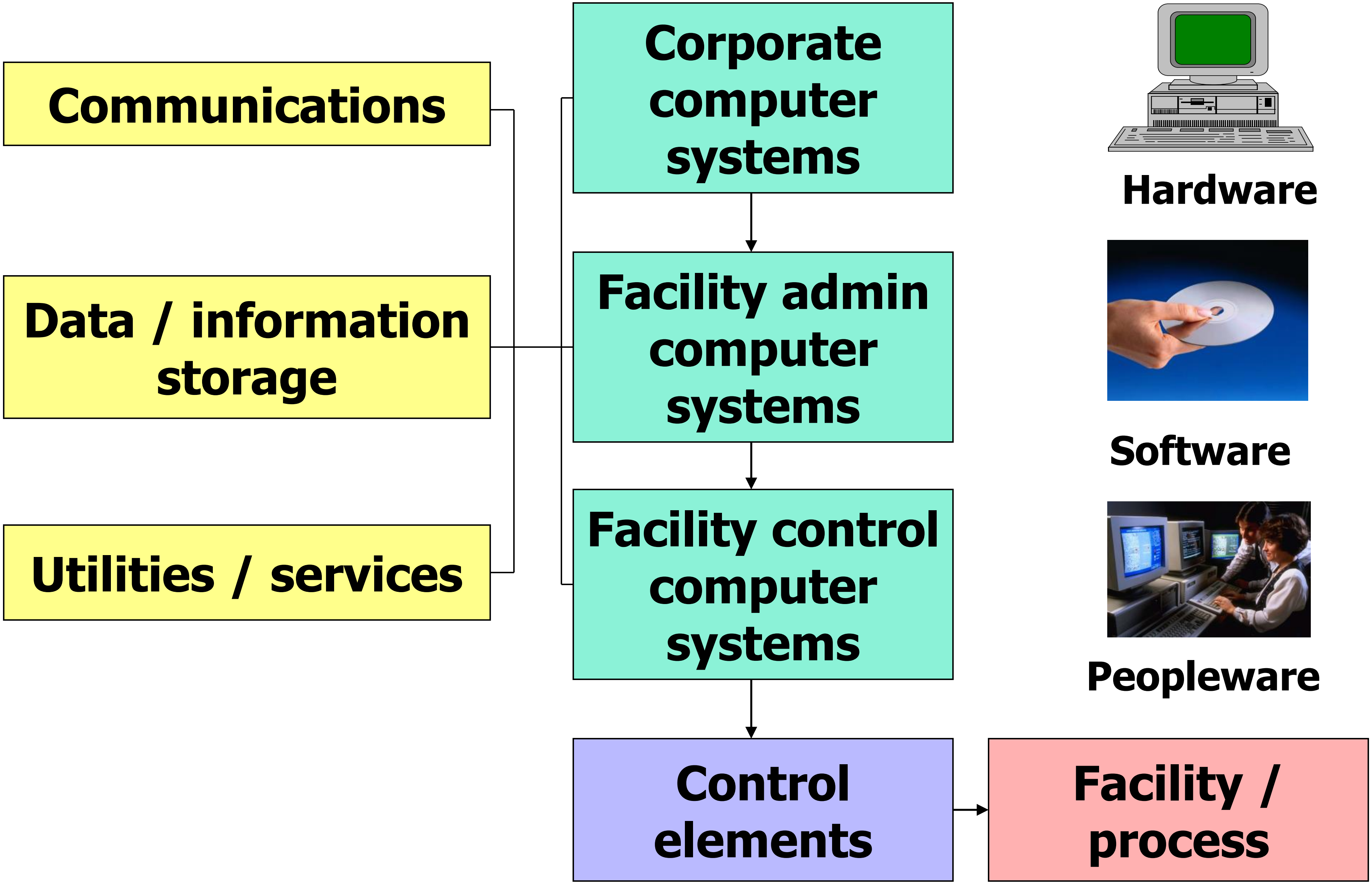


CYBER SECURITY FOR MANUFACTURING AND PROCESS PLANTS

ASSETS	INTENTS
Stored information	Obtain, corrupt, damage, destroy or prohibit access
Computer systems	Disable
Controls	Manipulate



PROTECTION OF COMPUTER SYSTEMS



Communications

Data / information storage

Utilities / services

Corporate computer systems

Facility admin computer systems

Facility control computer systems

Control elements

Facility / process

Hardware

Software

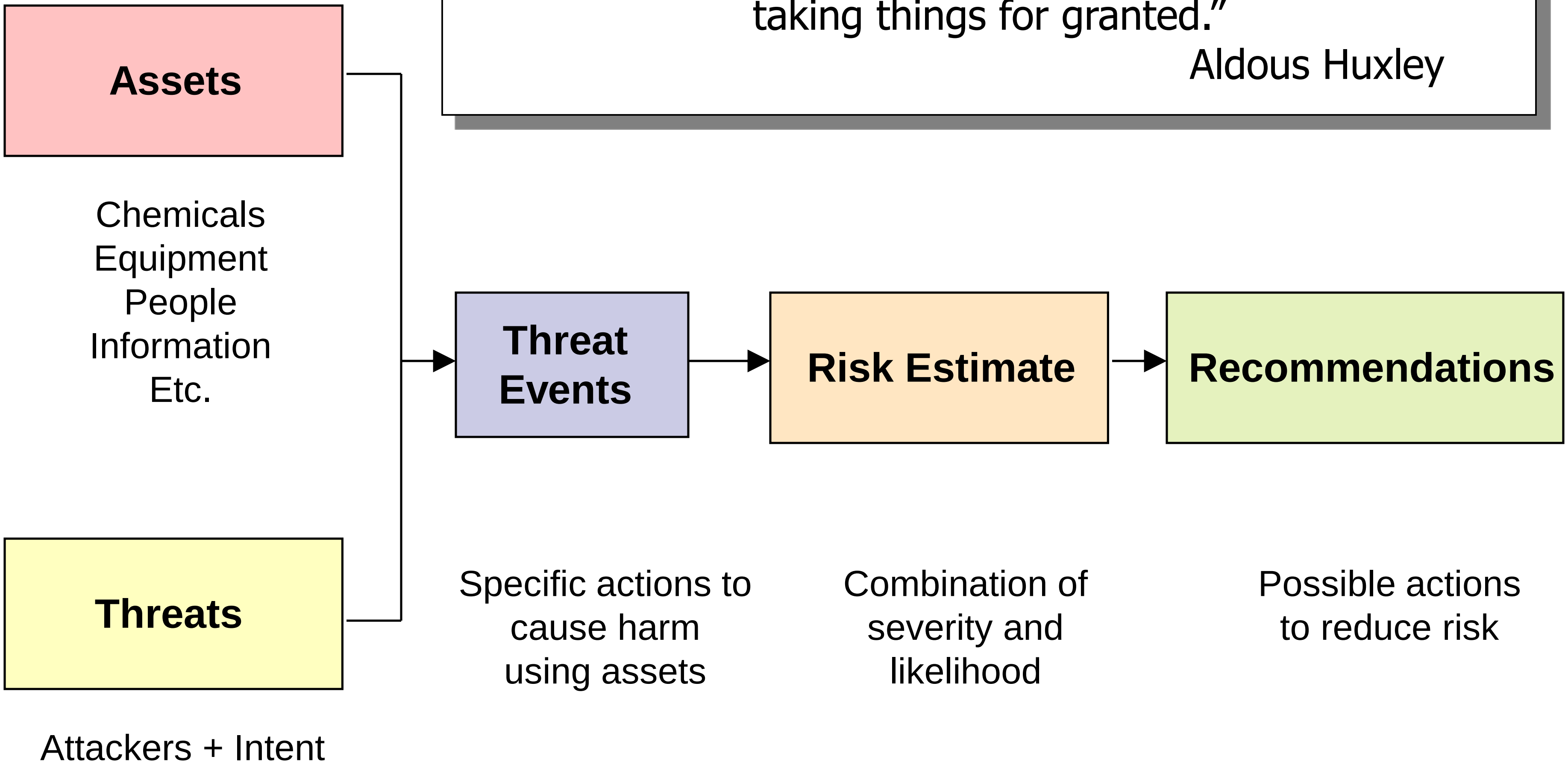
Peopleware

MANAGING CYBER SECURITY

- American Chemistry Council's (ACC's) Responsible Care® Security Code of Management Practices
  - Requires ACC members to perform cyber SVAs for their facilities
  - Part of a risk-based management system

MODEL FOR SECURITY RISK ASSESSMENT

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



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

COMPUTER SYSTEMS TO CONSIDER

- Manufacturing and process control
- Production management
- Safety systems operation
- Access control
- Information storage
- Data historian
- Financial systems
- Order entry
- Inventory management
- Warehousing
- Maintenance
- E-commerce
- Communications
- Power and other utilities
- Transportation
- Etc.

POSSIBLE ATTACKERS - INTERNAL

- Disgruntled employees
- Former employees
- Contractors
- Vendors
- Customers
- Visitors
- Etc.

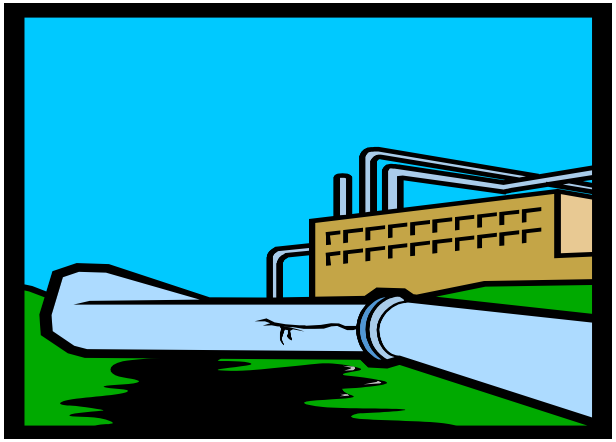
POSSIBLE ATTACKERS - EXTERNAL

- Hackers
- Terrorists
- Criminals
- Competitors
- Activists
- Etc.

POSSIBLE INTENTS

- Damage
- Destruction
- Disruption
- Denial of use
- Theft
- Diversion
- Manipulation
- Contamination

- Spoiled products
- Shutdown
- Release
- Fire
- Explosion
- Runaway reaction
- Etc.

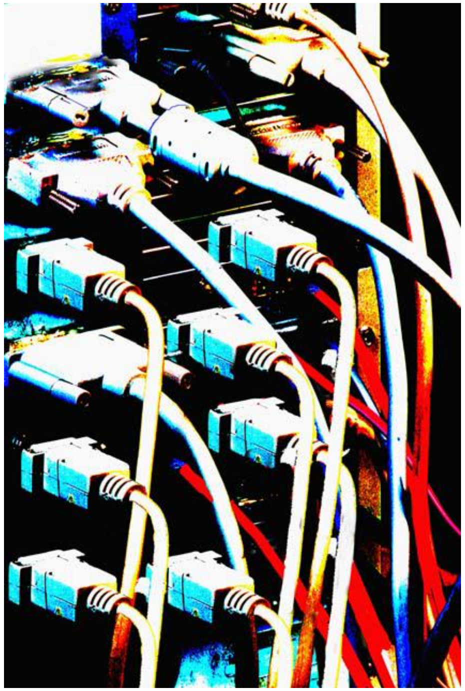


SECURITY VULNERABILITY ANALYSIS (SVA)

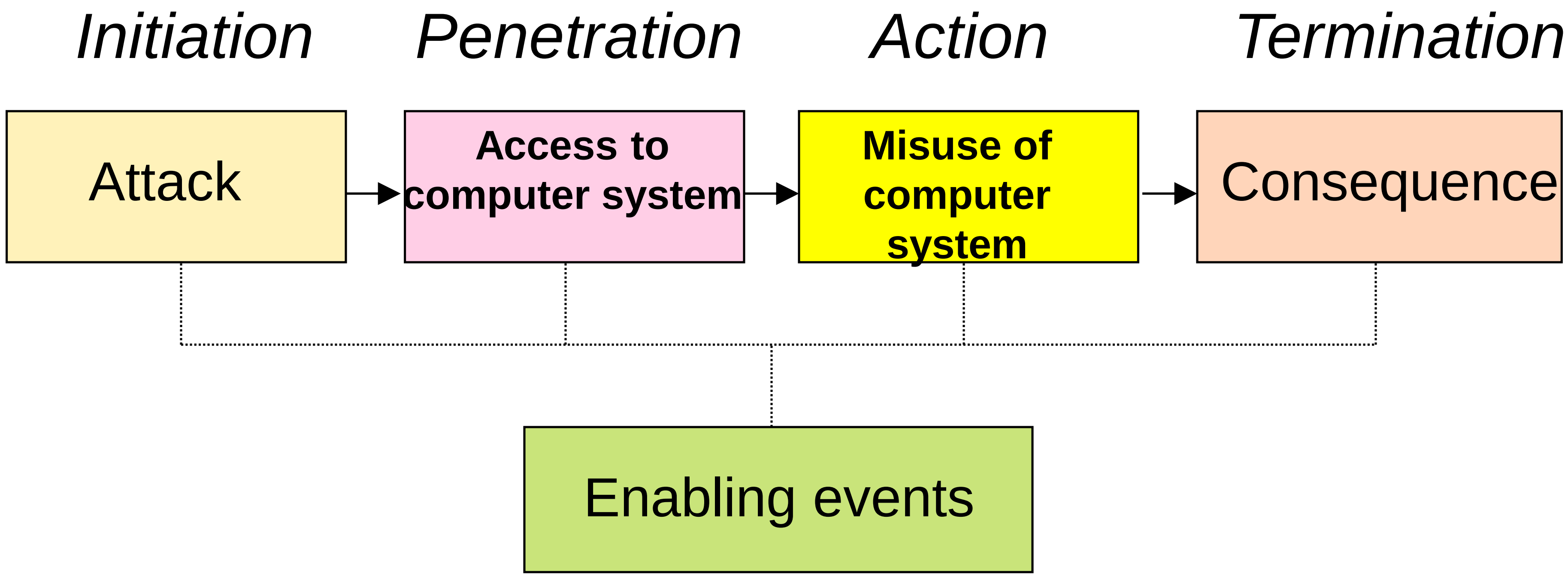
- Identifies ways in which deliberate acts could cause harm (*threat scenarios*)
  - How flaws or weaknesses expose a system to attack

VULNERABILITIES IN COMPUTER CONTROL SYSTEMS

- Network access
- Dial-up modems
- Unauthorized HMI use
- Wireless networks
- Partner networks
- Inadequate physical protection
- Unattended workstations
- Accessible cabling
- Etc.

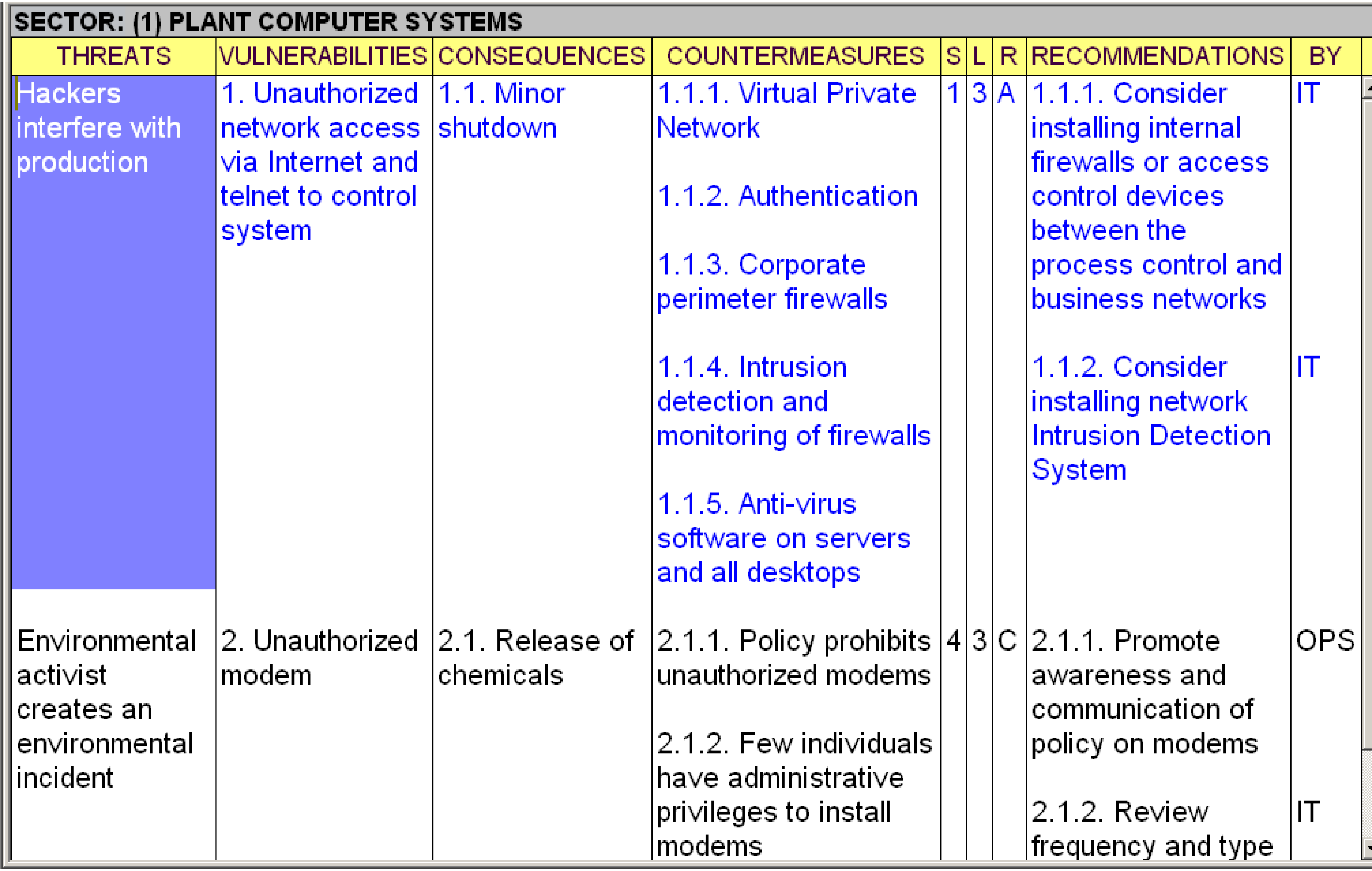


ELEMENTS OF A CYBER THREAT SCENARIO



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

CSVA-SB WORKSHEET

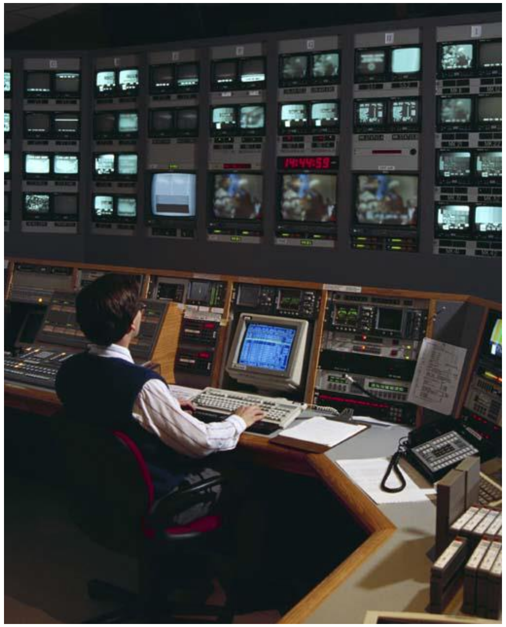


SECTOR: (1) PLANT COMPUTER SYSTEMS

THREATS	VULNERABILITIES	CONSEQUENCES	COUNTERMEASURES	S	L	R	RECOMMENDATIONS	BY
Hackers interfere with production	1. Unauthorized network access via Internet and telnet to control system	1.1. Minor shutdown	1.1.1. Virtual Private Network 1.1.2. Authentication 1.1.3. Corporate perimeter firewalls 1.1.4. Intrusion detection and monitoring of firewalls 1.1.5. Anti-virus software on servers and all desktops	1	3	A	1.1.1. Consider installing internal firewalls or access control devices between the process control and business networks 1.1.2. Consider installing network Intrusion Detection System	IT IT
Environmental activist creates an environmental incident	2. Unauthorized modem	2.1. Release of chemicals	2.1.1. Policy prohibits unauthorized modems 2.1.2. Few individuals have administrative privileges to install modems	4	3	C	2.1.1. Promote awareness and communication of policy on modems 2.1.2. Review frequency and type	OPS IT

LESSONS LEARNED - CSVA

- Analyze corporate computer systems first and separately
- Approaches familiar to plant personnel work best
  - Scenario-based



LESSONS LEARNED – CSVA (CONTD.)

- Facility subdivision
  - Treat each manufacturing process since vulnerabilities and consequences of attacks will vary
  - Useful to take each control system and analyze the various parts of the process it controls
- Recognize commonalities between control systems and processes but also address differences
  - Avoid repetition

LESSONS LEARNED – CSVA (CONTD.)

- Consider addressing unintentional attacks
  - Often mentioned by CSVA team members
  - May not have been addressed in PHAs
- Also, consider addressing physical attacks
  - Sometimes not addressed in physical SVAs or only to a limited extent
- Consider dividing insiders into “highly skilled” and “normal skilled” groups

LESSONS LEARNED – CSVA (CONTD.)

- Sometimes obvious countermeasures have not been taken, e.g.
  - Screening personnel
  - Firewalling control systems
  - Air gapping safety instrumented systems
  - Eliminating or controlling/securing modems
  - Using dumb terminals
  - Managing portable computer storage media
  - Etc.
- Initial self-assessment using checklists is valuable

LESSONS LEARNED – CSVA (CONTD.)

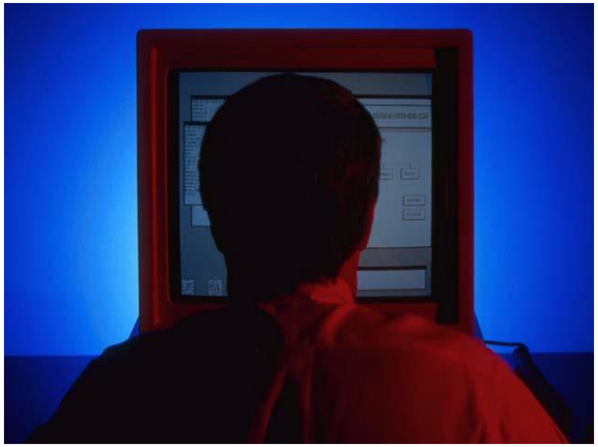
- Countermeasures must be acceptable to affected parties for them to be successful
  - E.g. process operators may be unwilling to use passwords
- Countermeasures must also be compatible with the existing facility
  - E.g. a desired new intrusion detection system may not be capable of implementation on a legacy system

LESSONS LEARNED – CSVA (CONTD.)

- CSVAs create a new awareness of cyber security for participants
- Studies help companies develop policies for implementation of new systems
  - Learn from mistakes found by performing CSVAs

LESSONS LEARNED – RISKS

- Risk from internal threats is often high
  - Ease of access
  - Lack of controls
  - Knowledge of personnel
  - Target likelihood



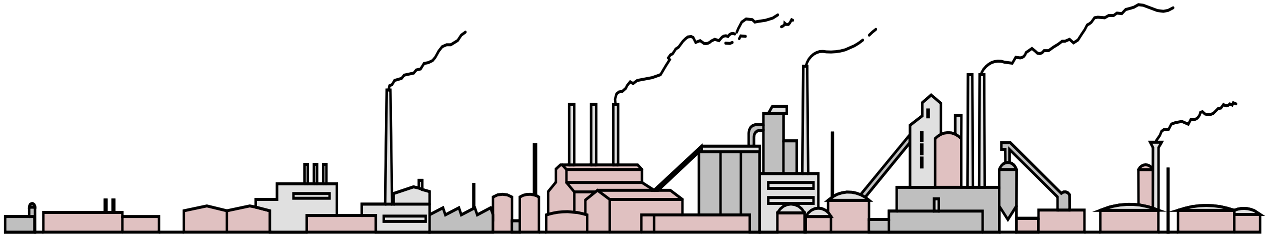
- Access controls are vitally important
- Inadequate physical protection of cyber facilities is not unusual
- Importance of basic protection measures such as firewalls for control systems has been recognized
  - Still awaiting implementation in some cases

LESSONS LEARNED – ENABLERS

- Lack of awareness by management and plant personnel
- Infrequent changes in network access controls
- Use of unauthorized storage media, files and programs

SUMMARY

- Significant number of CSVA studies has been performed
- Many more studies will be performed in the future
- Lessons learned from initial studies should be shared
  - Help ensure efficient and effective future use of CSVA methods



FURTHER INFORMATION

- Technical papers on cyber and process security:

  www.primatech.com

- Contact info:

  paulb@primatech.com

OTHER LESSONS LEARNED – CSVA

- Team membership
  - Process engineer and network / control system engineer are key participants
- Key reference documents
  - Process drawings and computer system diagram
- Use a standard format for CSVA worksheets and reports

OTHER LESSONS LEARNED – CSVA (CONTD.)

- Use standardized checklists to assist the analysis
  - Attackers
  - Intents
  - Vulnerabilities
  - Consequences
  - Countermeasures

OTHER LESSONS LEARNED – CSVA (CONTD.)

- List global countermeasures separately
- Risk ranking scheme should provide sufficient discrimination between scenarios
- Duration of studies averages a few hours per process