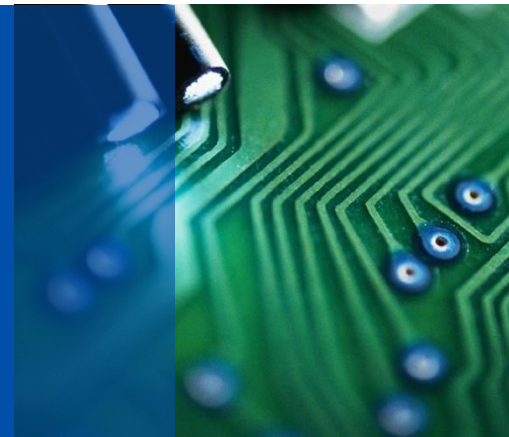




# Process Control Networks Risk Assessment



**Gypsy Morinelli, CISSP**

**Network Infrastructure and Security Team Leader  
Chevron Pipe Line Company**

# TOPICS

- Objectives of a Risk Assessment
- PCN Risk Assessment Model
- Risk Assessment Approach
- Risk Assessment Steps

# Risk Assessment Objective

## Purpose

To determine high risk security vulnerabilities in systems, processes, applications, and tools (purchased or developed) and to determine adequate controls necessary to reduce or to remove the risks inherent with the vulnerabilities found.

## Outcome

- Risk Assessment Summary
- Suggested actions to handle risks
- Criticality Validation ( CIA Ratings)

# CIA+E: Confidentiality, Integrity, Availability + Environment

Information Protection efforts should be prioritized based on business needs for Confidentiality, Integrity, and Availability PLUS risks of the information Environment (CIA+E)

## Confidentiality (was Data Sensitivity)

- Authorized access only
- Prevent release of data

## Integrity (was Application Type)

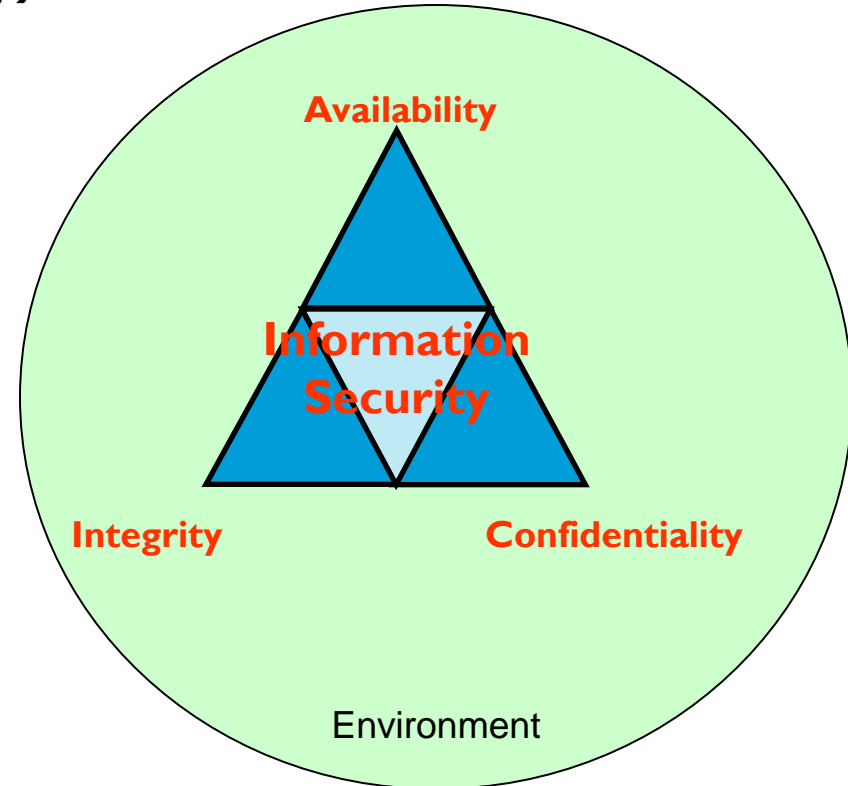
- Prevent unauthorized deletion
- Prevent unauthorized alteration

## Availability (was App Criticality)

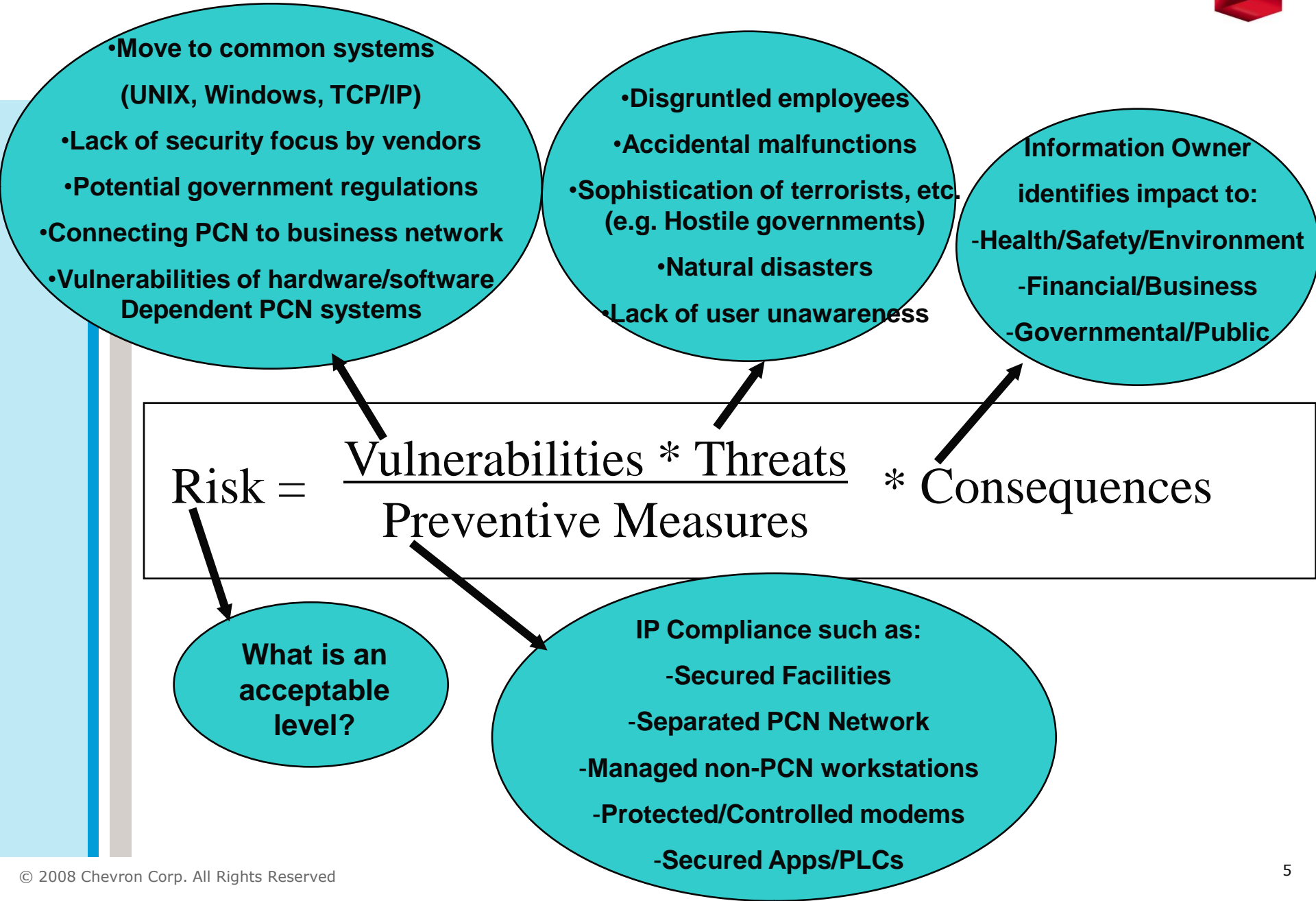
- Prevent degraded services
- Prevent denial of service

## Environment

- Understand risk based on location of assets



# PCN Risk Assessment Model



# Risk Assessment Approaches

## 1. Technology based

- Firewall/Router assessment
- Server configuration assessment
- Wireless assessment

## 2. System based

- SCADA system risk assessment
- PCN risk assessment

# Step 1

## Identify The Scope Of The Assessment

- Limit scope to components of a single system:
  - A single PCN application.
    - ▶ Utility, field, and SCADA system likely each would have a separate assessment
- Collect basic information about the system:
  - System Name and System Type
  - Identify all the components of the system
    - ▶ Servers, OS, software packages, etc.

## Step 2

# Identify Participants

- Impact Assessment should involve people knowledgeable of PCN operations, configuration, and IT Technologies and associated risks. For Example:
  - SCADA/DCS Engineer
  - Operations Supervisor, Head Operator, etc.
  - IT Analysts for SCADA application, server, network
  - Vendor
  - Operations management
  - Application/system steward
  - Application/system administrators
  - Security Analyst
- Use a facilitator with PCN compliance SME knowledge to facilitate the workshop, like:
  - Security Consultant

# Step 3

## Identify vulnerabilities and scenarios

- Identify vulnerabilities related to five components of the PCN:
  - Environment: Roles & Responsibilities, General Compliance, Facilities, Employees, Processes, etc.
  - Network/Communications: Compliance, Management, Separation, non-PCN machines, Radio, Satellite, Wireless, modems, Controls.
  - OS (servers/workstations): Compliance, Management, patching, Controls, Anti-Virus
  - Applications: Compliance, Management.
- Identify data confidentiality
  - Is the information contained considered Intellectual property?  
Does it contain sensitive or personal data?
- Following scenarios will help identify availability and integrity values

# Scenario 1

## Hacker Attack



### **Scenario 1: Hacker has gained control of PCN system**

- The hacker could be any unauthorized user, which may include disgruntled employees or contractors who are knowledgeable of the system (local hackers) or persons on the business/other connected networks or someone in an internet café on the other side of the world.
- It is important to assume you are not aware and that the hacker is knowledgeable of the systems and how to implement a worst case attack.
- Assume the hacker has penetrated the PCN firewalls and IS ON YOUR PCN.... now what's the impact?

# Scenario 2

## Server/Workstation disabled



### Scenario 2: PCN Servers/Workstations are disabled

- The Control Room and/or the PCN Servers/Workstations could be disabled for various reasons:
  - Electrical outage could disable all servers/workstations not protected by UPS
  - Hardware failure of a single server/workstation is very common
  - Fire/Flood could impact the entire control room and/or PCN servers/workstations
  - Virus/worm would normally have the wide ranging impact
    - ▶ MS Windows servers/workstations could all be disabled at the same time
    - ▶ Unix/Linux has low risk of virus/worm

# Scenario 2

## Server/Workstation disabled (cont.)

### Scenario 2: PCN Servers/Workstations are disabled

- Calculate likely outage (e.g. based on availability of parts, etc.)
- Calculate a worst (probable) case impact considering :
  - Outage happened at worst possible time (e.g. can't shutdown safely, etc.)
  - Outage is extended (e.g. shutdown and start-up times are normally very long, etc.)
  - The control room went blind and the operations manager shut down the facility (based on existing practices)
  - Ability to transition to manual or partial. (e.g. need to call off-site support like during holidays, etc.)

# Scenario 3

## Network Disabled



### Scenario 3: Modem and/or Network Disabled

- Assume all modems and/or networks have been disabled, which prevents communications between the PCN server and Controllers. For example,
  - Network scan results in network being flooded - grinding to halt
  - Fire/flood has damaged network devices
  - War dialing is run continuously to make modem phone lines busy
- Determine impact based on what could potentially occur and ability to respond
- Ability to respond should be based on ability to transition to manual operations or shut down the plant, and also the worst case scenario:
  - Network engineers need to be called out (delayed arrival)
  - Effective restore procedures and obtaining configuration backups
- Consider the ability of the PCN application to warn the operator if the network or polling is disrupted

## Step 3 (cont)



- At the end of this step you will have an understanding of your CIA requirements and the impact of security breaches associated with the PCN.
- Then look at your processes and mitigating and compensating controls in your area (i.e. architecture and configuration of your network -defense in depth-, process to control shared accounts, process to harden your systems, patching processes, change management, network monitoring, etc.)

## Step 4: Summary - Develop Recommended Actions

- Based on your scenario impact results and your mitigating and compensating controls, develop a set of recommended actions
- Record specific action plans on what you will do to remediate the gap.
- When developing the action / strategy to remediate be specific to the Facility / PCN in question, priorities would be driven by the criticality and mitigating controls in place or in the plans.

# Step 5

## Summary and Implementation

- Present the summary of risks along with recommended actions for consideration
- Work with management to obtain guidance / approval
- Schedule and Implement Changes:
  - Plan and fund implementation of controls
  - File Exceptions when appropriate
  - Monitor progress of implementation efforts
  - Update PCN Risk Assessment based on changes

## Next Steps : Sustain security

- Update operating procedures to support change to PCN controls
  - Operate the PCN system with these new controls
- Review PCN risk assessment every time a significant change occurs on your process control network to reflect state of the PCN system as it evolves

## Tools available

- Nessus and Bandolier policies developed by Digital Bond
  - <http://www.tenablesecurity.com>
- CSET – Cyber Security Evaluation Tool form the Department of Homeland Security
  - [http://www.us-cert.gov/control\\_systems/satool.html](http://www.us-cert.gov/control_systems/satool.html)

# Questions?

