



# Emerging Risk Assessment Options

## API Pipeline Conference & Cybernetics Symposium 2010

Annie McIntyre  
Principal Member of Technical Staff  
Sandia National Laboratories  
21 April 2010



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.





# Topics

- Background & Purpose of a Risk Assessment
- Components of Practical Methodologies
- Common Approaches
- Concerns for the Future
- Cost Considerations



# Background



# Purpose of a Risk Assessment

- Mitigate risks that threaten successful operations (safety, security, business)
- Increase preparedness and resilience
- Better position your operation to resist and survive adversity





# Effectiveness of Historical Methodologies

- Historical precedence for complex systems in many sectors
- Continual relationship between value and risk
- Risk assessments are validated

## Example: Evolving Military Risk Methodologies

*CARVER – Special Forces Vietnam – mission risk, target values*

*DSHARPP – target ranking with quantitative values*

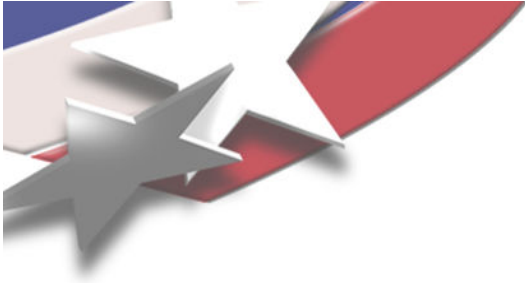
*MSHARPP – asset and infrastructure protection*

*Subjective or Relative Rankings*

*vs*

*Hard Values*





# Risk Assessment Process

- Threat Assessment
  - *Who or what can cause damage*
  - *Why would they want to do damage*
  - *The tools or perspective necessary to do damage*
- Vulnerability Analysis
  - *Where are the weak spots*
- Consequence Definition
  - *What are the immediate effects*
- Business Impacts Conclusions
  - *What are the damages*
- Mitigation
  - *What fixes are necessary*
- Life-cycle Application
  - *Long term prevention*



# Purpose of Understanding Your Risk

- Enable the development of strategies for preventing, detecting, mitigating, and recovering from cyber-security incidents with focused and defined objectives
- Provide a strong basis for both decision making and improvements with realizable, specific outcomes
- Help to clarify and prioritize security concerns for the industry, making implementation less overwhelming



# Overarching Objectives

- Using guided principles to determine what is valuable to your organization
- Ranking high-level goals
  - Safety
  - Security
  - Continuity of operations
  - Financial consistency
- Keep goals in focus when developing a risk assessment approach



# Customized Goals

- What are the aspects of a risk assessment that can meet your overarching goals?
- A defined approach
  - By Location (Substation X)
  - By Function (Application or Platform X)
  - By Threat (Capabilities of Bad Guy X)
  - By Birds-Eye View (Where are the Weak Spots?)
- A risk assessment has guiding principles but it is what you make it....no 'one size fits all'.

*Result: A clear picture of asset value, vulnerabilities, and required mitigations.*



# Components of Practical Methodologies



# Consistent Definition of Risk

- The components of risk are
  - Threat
  - Vulnerability
  - Consequence

$$\begin{array}{ccccccc} \text{THREAT} & \times & \text{VULNERABILITY} & \times & \text{CONSEQUENCE} & = & \text{RISK} \\ \text{Resources} & & \text{Weaknesses} & & \text{Effect} & & \text{Business Impact} \end{array}$$

- Risk exists in all facets of business and operations
- While an organization will never be able to logically remove all risks, it can “live through” adverse situations



# Elements of an Assessment

In its simplest form....

- Establish objectives
- Define an approach
  - Assess threat and vulnerabilities
  - Identify assets
- Use tools and techniques
  - Design reviews
  - Red, blue teaming
  - Penetration testing
  - Consultation
- Determine results and findings
  - Calculate your risk
- Apply mitigations



# Quantitative and Qualitative Options

- Quantitative Values
  - Statistics and Probability
  - Known or historical values
- Qualitative Options
  - Relative rankings
  - Subjective values
  - Level of comfort and acceptable risk
- Options can depend on assessment objectives and relationship to cost
- Quantitative options can resonate when making the business case for an assessment



# Establishing Boundaries

- Boundaries in an assessment can help establish meaningful results.
- Two aspects must be considered:
  - Physical Security
    - Access Control and Intrusion Detection
    - Authorization and Assigned Responsibility
  - Operational Security
    - Role of People and Processes
    - Supported by Policy
    - Consideration of “Realistic” Operations





# Defense in Depth Approaches

- Layered look at security
- Valuable for piecemeal approaches to security
- Assists in times of budget constraints
- Can occur at varying layers:
  - Application and functional
  - Node/Asset
  - System
  - Network Architecture
  - Human Interfaces
  - Operating Policies
- The onion approach





# Zero to Full Knowledge

How much information does your threat have?

- Zero to full knowledge approaches should support overall objectives
- Particularly useful in addressing specific threats such as insider and outsider
- Supports a defense in depth approach



# In-House vs Outsourced

- An internal, organizational risk team is valuable
- Cost considerations are key
- A choice should support overall objectives (i.e. application level assessment vs a policy review)
- Consider staff resources
- Maintain a realistic view
- Weigh the objectives in terms of zero to full knowledge testing



# Common Approaches

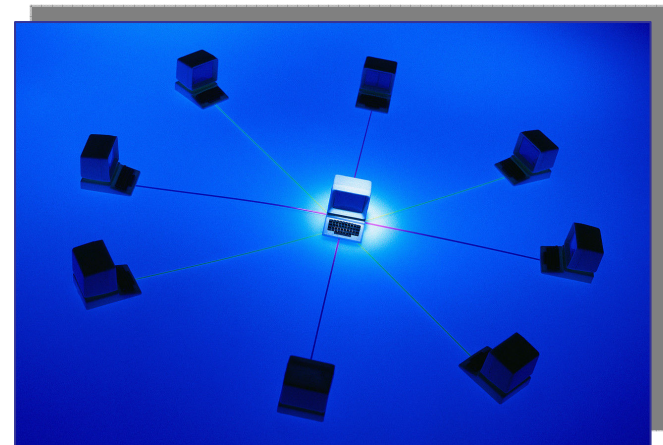


# Many Options

Many approaches can be combined or extrapolated based on primary objectives.

Examples:

- Paper reviews
- Design assessments
- Hands-on testing and analysis
- Red teaming
- Threat assessments
- Specific vulnerability testing
- Statistical approaches
- Modeling and simulation





# Tools and Processes

- Defined Processes and Methodologies

Examples:

- Sandia RAM

- $\text{Risk} = \text{PA} * (1 - \text{PE}) * \text{C}$ ,
- PA is the likelihood of adversary attack,
- PE is security system effectiveness,
- $1 - \text{PE}$  is adversary success, and
- C is consequence of loss of the asset.

- Matrikon RiskMAP

- Ranked risks in the business framework

- Compliance Assessments

- Certifications

- Align with best practices or standards
- Utilize govt guidance
- 3<sup>rd</sup> party



# Compartmentalized Approaches

- Objectives target one aspect or function within the system
  - Specific capability or element
  - Individual policies and procedures
  - In-house or outsourced
  - Can meet cost challenges, but can leave holes
- Specific threat assessments
  - Insider and outsider
  - Threat Matrix
  - Zero to full knowledge
  - Assumption based
  - Effective particularly in compartmentalized assessments





# Concerns for the Future



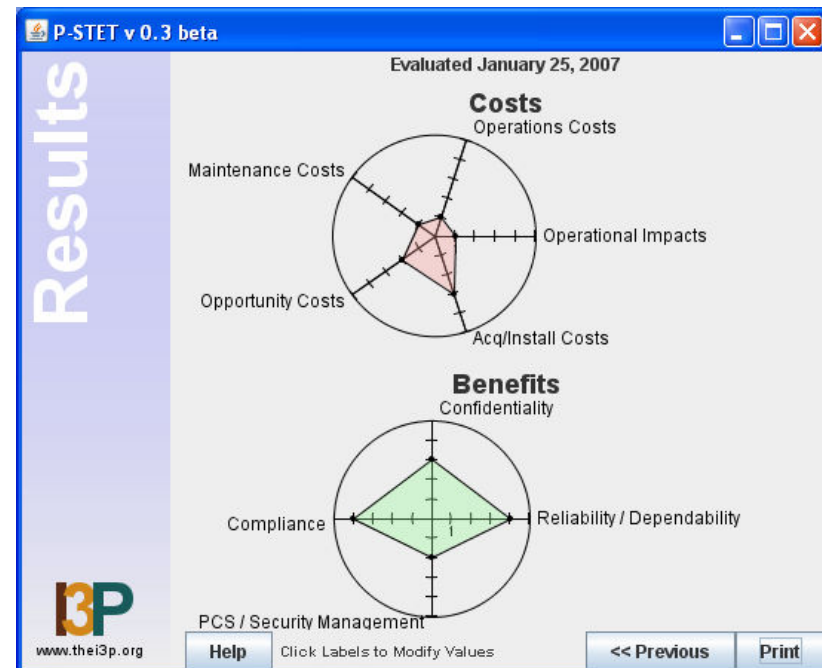
# Increased Interdependencies

- Always advancing cyber capabilities
- Increased interconnectedness at all levels
- Increased demand and availability in emerging architectures
- Remote connectivity
- Regulations and guidelines
  - Increased cyber interoperability
  - Reporting requirements
  - Evolving with energy policies and technology



# Financial Challenges

- Agreement on established objectives
- Justification of cost in a tough market
- Finding technical and economic common ground
- Weighing the cost of inaction
- Agreement on acceptable risk
- Procrastination until the market improves





# Cost Considerations



# Measuring the Risk of a Risk Assessment

- Larger costs to consider
  - Cost of preparing and conducting the assessment
  - Cost of mitigations and implementation
  - Life cycle considerations
- Cost of not addressing the risk
  - Technical and operational consequences
  - Safety, security, and quality of life consequences
  - Feed back to financial impacts



# Measuring the Risk of a Risk Assessment

- Probabilistic Approaches
  - Hard numbers are not always attainable or accurate
  - Can be useful with a management audience
- Working with what you have
  - Cost of downtime
  - Cost of a safety infraction
  - Cost of new equipment
  - Cost of training staff



# Return on Investment

- True ROI
  - Blend of quantitative and qualitative approaches
  - Value of better, future positioning
  - Similar to insurance market values
  - Confidence by the organization, public, shareholders
- Match to the definition of your Acceptable Risk
- Be prepared for future expectations by the industry, government, and shareholders





# In-House vs Outsourcing

- Considerations
  - Value of staff time
  - Cost of other resources and tools
  - Blending in-house and outsources as part of the defense-in-depth approach
  - The end goals and timeliness
  - Implementation of mitigations
- In a tough market, it can be a balancing act
  - Piece meal solutions and mitigations can add up
  - One-stop outsourcing for a large assessment can be costly
  - Hidden costs and challenges with an in-house assessment



# Summary



# Challenges Facing Pipelines

- A true critical infrastructure, product must flow to maintain US operations
- Critical customers
  - Military installations
  - Hospitals
  - Airports and Transportation systems
  - Urban *and* rural homes, etc.
- Geographically disparate
- Above and below ground systems
- Impossible to physically protect thousands of miles of pipe
- Attractive targets (transmission and distribution)
- Already facing varying threats – hurricanes, activists, etc
- Differing activities (safety, security) overseen by different agencies (TSA, DOT, Coast Guard)



# The Reality

- Challenges and realities exist in meeting the business and operational needs of industry today.
  - Interconnectivity
  - Technical Challenges
  - Standards, Policies, and Regulations
  - Application of Mitigation Strategies
  - Communication and Organizational Culture
  - Identifying Objectives and Meeting End Goals
- Success requires a comprehensive approach that includes:
  - Communication inside the organization
  - Decision making, weighing technology and cost
  - Making the technical and financial case for investing in security



# Search Tips

- Sample Search Keywords
  - Quantitative/Qualitative Risk
  - Risk Assessment, Risk Analysis
  - Cyber Risk
  - Threat Assessment
  - Risk Assessment Methods
  - Risk Assessment Tools
- Documents
  - NIST guidance
  - DOE 21 steps
  - API Standards
  - TSA guidance
- Feedback from Industry Members
- Ask Questions to Industry Forums

Annie McIntyre  
Energy Systems Analysis  
Sandia National Labs  
[amcinty@sandia.gov](mailto:amcinty@sandia.gov)  
(505) 284-0968



# Backup



# Technical Vulnerabilities

- Implementation vulnerabilities: a component or system includes flaws as part of its software or hardware that compromise its security
- Examples:
  - Classic programming flaws, e.g. buffer overflows
  - Non-secure microcode in embedded systems
  - Accidental exposure of key security data
  - Compromised cryptographic modules that reduce their security
- If known, implementation issues can be patched or wrapped
- Often, these are unknown, so their mitigation requires vigilance and defense-in-depth



# Technical Vulnerabilities

- Configuration vulnerabilities: components that could provide adequate security are poorly configured and installed
- Examples:
  - Firewalls installed using “out-of-the-box” configurations
  - Vulnerable ports left open mistakenly
  - VPN configured for authentication rather than confidentiality
  - IDS is installed with vulnerable network interfaces
  - An incorrect or unsuitable product is applied
- These are detectable through system scanning and/or audit
- Repair is relatively straightforward



# Operational Vulnerabilities

- Bypassing required security controls to ease the use of devices / subsystems
- Examples:
  - Setting a field system to never screen lock
  - Shared accounts
  - Weak, easily-guessed authentication phrases
  - Workarounds for security perimeters
- These should be forbidden by security policy and system security plans
- Amelioration is often similar to configuration vulnerabilities



# Physical Vulnerabilities

- Physical security of cyber assets reduces system security
- Examples:
  - Shared wiring or equipment spaces
  - Poorly secured or monitored physical security perimeters
  - Opportunities for unauthorized personnel to interact with secure cyber assets
- Mitigations require adequate physical security engineering, particularly addressing key cyber assets



# Organizational Vulnerabilities

- Lack of definition or shared views
  - What are the organizational objectives? Safety, security, public perception
  - Does security include people, processes, and technology?
  - Is there a security plan with defined policies?
  - Does each person understand their role and responsibility in security?
- Communication is vital in security
- Financial backing of decisions regarding security
- The mindset that prevents security from overarching across operations
- History



# Characterized Vulnerabilities (From Industry)

<b>Vulnerability Category</b>	<b>Description and Examples</b>
System Data	<ul style="list-style-type: none"><li>• Lack of understanding of what data is considered sensitive, how it should be separated and protected.</li></ul>
Security Administration	<ul style="list-style-type: none"><li>• Lacking policies, standard procedures, training, and corporate/industry security plans.</li><li>• Formal configuration management needed for upgrades, legacy plans, and patching.</li></ul>
Architecture and Design	<ul style="list-style-type: none"><li>• No integrated security in PCS designs. Security must be an add-on.</li><li>• Centralized storage or control mechanisms are single points of failure.</li></ul>
Platforms	<ul style="list-style-type: none"><li>• Patching, backups, passwords, OS security, application security, and security policies for access control and file sharing are needed.</li><li>• Physical access control is lacking.</li></ul>
Networks and Communications	<ul style="list-style-type: none"><li>• Wireless security, monitoring, encryption, access control, boundary security, and standards for implementation are needed.</li></ul>
Incident Response and Handling	<ul style="list-style-type: none"><li>• Response plans are lacking, as well as backup and disaster recovery plans.</li><li>• Forensic data collection and analysis is needed.</li><li>• Redundant operational capability is beneficial.</li></ul>



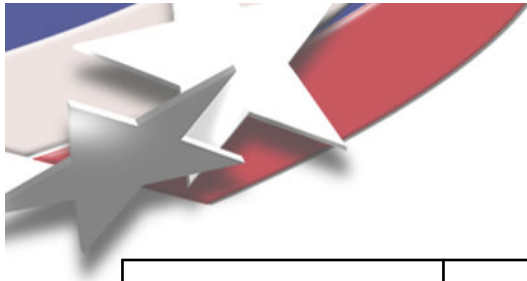
# Possible Technical Effects of Vulnerabilities

- Access control and authorization compromised
- Ability to escalate privileges
- Ability to hijack traffic, capture data
- Possible control of systems, applications, or network
- Installation opportunities
- Information gathering
- Ability to traverse the network with potentially unlimited bounds
- Data theft



# Possible Consequences and Impacts:

- Downtime
- Damage and repair costs
- Recovery resources
- Community's loss of a critical infrastructure for an extended period
- Damaged image or partnerships
- Environmental damage or fines
- Worker or public injury
- Value of stolen corporate trading information
- Value of stolen personnel data
- Value of altered commodity purchasing data
- Value of altered customer billing information



# Consequences & Resulting Impacts (From Industry)

Consequence	Effect	Impact
Access/Read/ Alter Data	<ul style="list-style-type: none"> <li>• Theft or alteration of corporate/industry data</li> <li>• Theft or alteration of critical operations data used for future attack</li> <li>• Theft of personnel data</li> <li>• Divulge corporate trading partner info</li> <li>• Billing and purchasing data changed</li> </ul>	<ul style="list-style-type: none"> <li>• Quality of life (i.e. identify theft, negative publicity for corporate and industry)</li> <li>• Physical impacts to equipment</li> </ul>
Gain Control of PCS Systems	<ul style="list-style-type: none"> <li>• Full operation of control systems</li> <li>• Can alter, stop, or destroy equipment and operations</li> </ul>	
Denial of Service	<ul style="list-style-type: none"> <li>• Halt operations on process control, business systems, or telecommunications</li> </ul>	
Access Systems as Jump-points	<ul style="list-style-type: none"> <li>• Use systems as part of a large scale, coordinated attack</li> </ul>	
Physical Access to PCS Systems	<ul style="list-style-type: none"> <li>• Can physically damage systems</li> <li>• Access as a trusted insider if electronic access controls are not in place</li> </ul>	
Introduction of a Virus/Worm	<ul style="list-style-type: none"> <li>• Can slow or halt operations</li> </ul>	