Implementing Security in a Multinational Environment

- a case study for bhpbilliton

plantdata technologies
a Division of Verano

Jonathan Pollet, CAP, CISSP

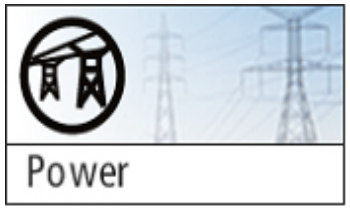
2006 ICSSS Coordination Workshop

August 2006

About PlantData Technologies

- Founded in 2001; Privately held consulting firm
- Founder Jonathan Pollet recognized leader in SCADA Security
- Headquartered in Houston, TX
- 10-year history of providing process control, SCADA, software development, integration and security solutions
- More than 40 global customers
- More than 100 service deployments
- Leading provider of SCADA Professional Security Services
- Joined with Verano in January 2006 to Capitalize on Similar Market Focus

PlantData Vertical Markets



- Generates power and provides network management of power transmission and distribution

- Monitors the transportation of millions of barrels of refined oil through miles of pipelines

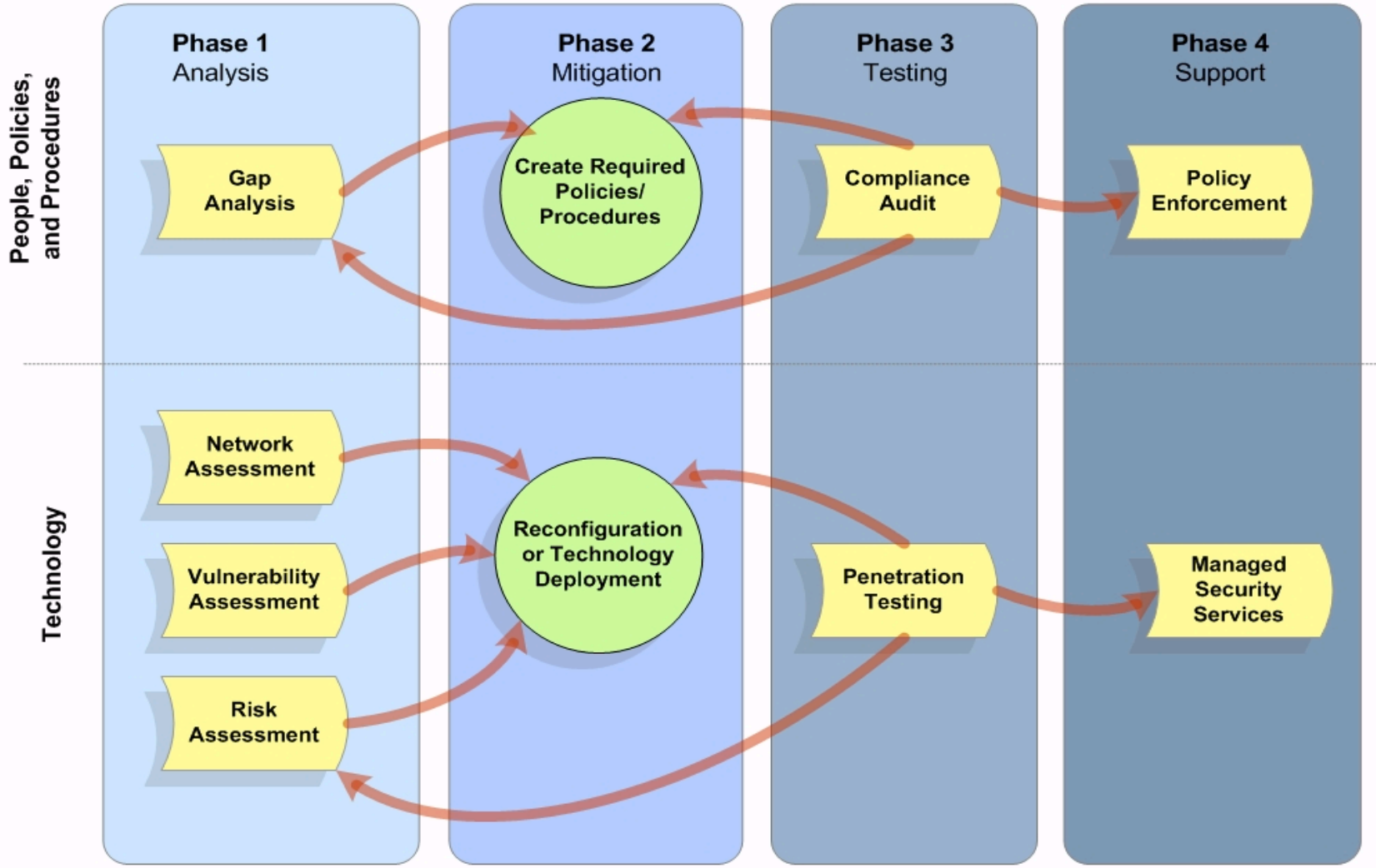
- Manages and controls railways, subway systems and airport facilities

- Distributes and purifies drinking water and provides environmental monitoring and supply management

Overview of Presentation

- Concept of Security as a Lifecycle
  - Analysis
  - Mitigation
  - Testing
  - Maintain
- BHP Billiton Corporate Overview
- Custom SCADA Security Roadmap for BHP Billiton
- Phase 1 - Define the Corporate Standard for SCADA Security
- Reference International, US, and Corporate Standards
- Standardized “Site Survey” used to Compare Facilities
- Remaining Phases in Roadmap
- Conclusion
- Comments?

Security Life Cycle

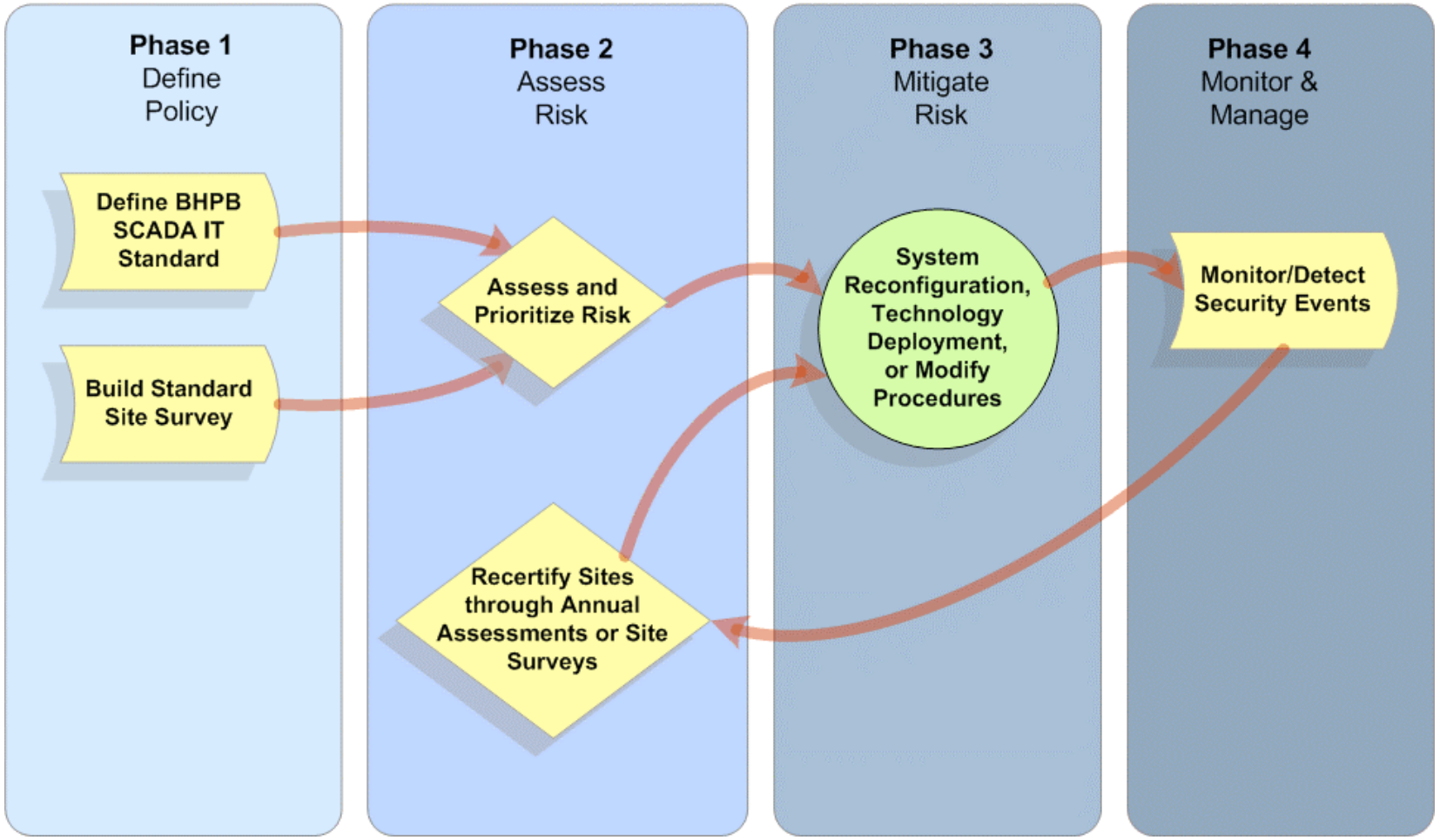


BHP Billiton Corporate Overview

- World's largest diversified resources company
- More than 100 operations in more than 25 countries
- Leaders in major commodity businesses including aluminum, energy coal and metallurgical coal, copper, manganese, iron ore, uranium, nickel, silver and titanium minerals, and have substantial interests in oil, gas, liquefied natural gas and diamonds.
- Required an internal corporate SCADA IT Guidelines that incorporated applicable International standards

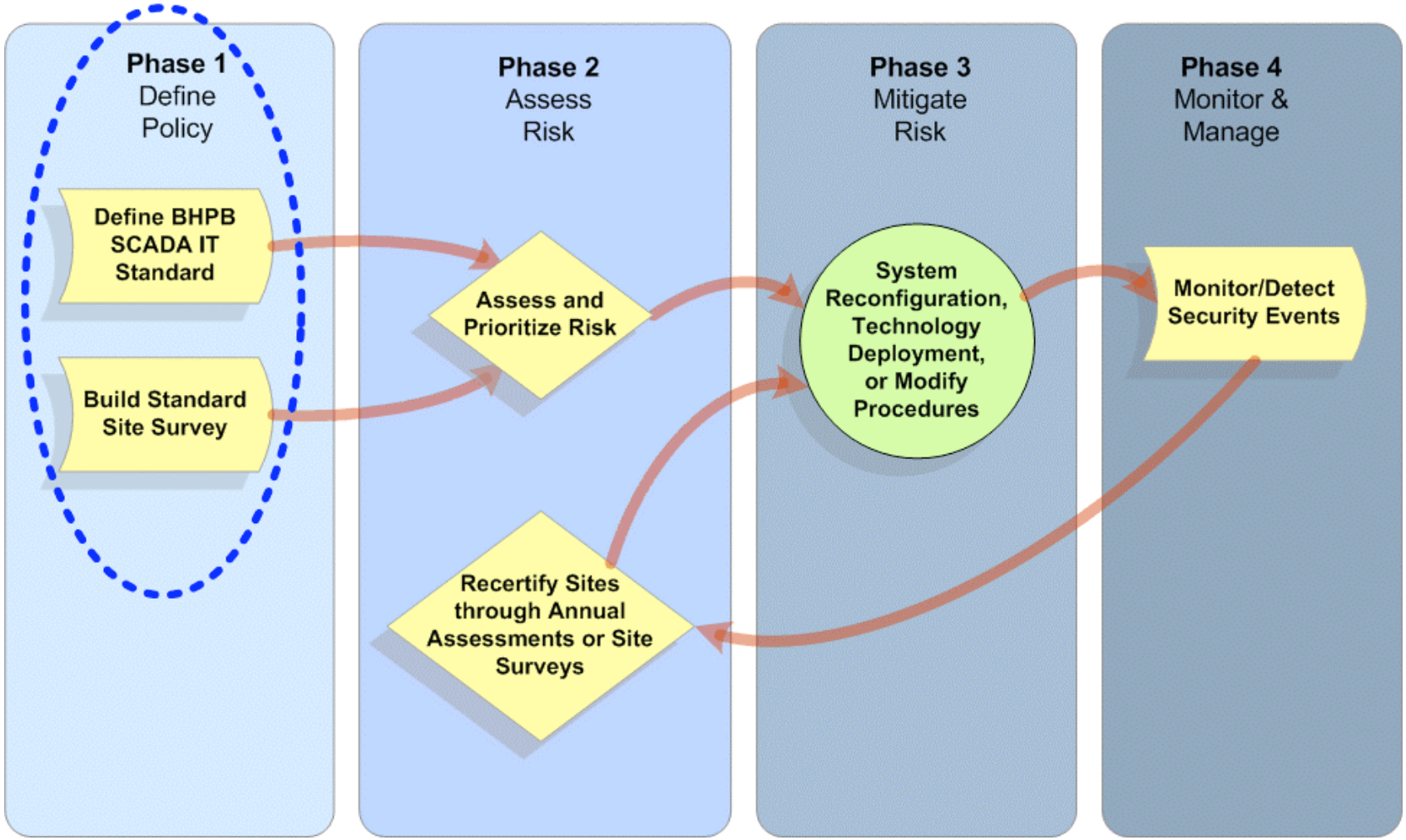
Custom SCADA Security Roadmap for BHP Billiton

BHBP SCADA Security Lifecycle



Phase 1 - Define the Corporate Standard for SCADA Security

BHBP SCADA Security Lifecycle



Reference International, US, and Corporate Standards

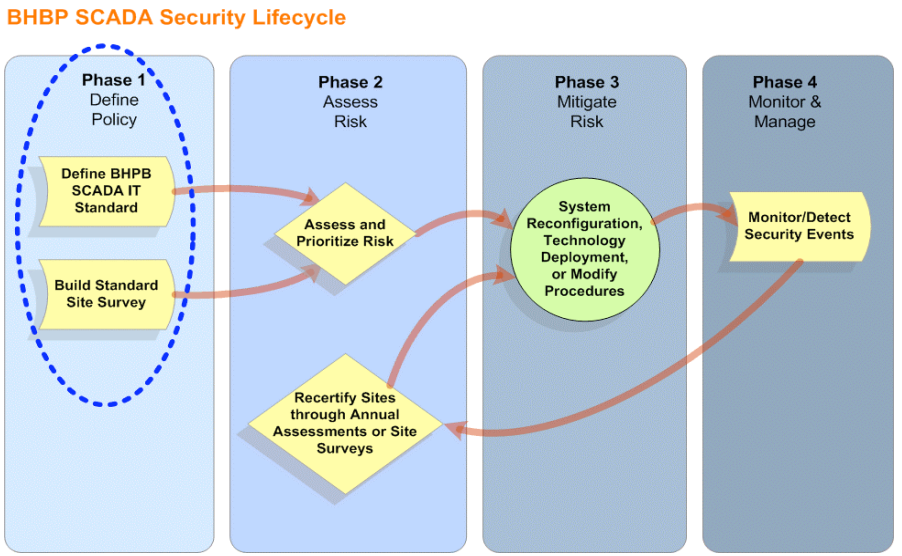
- ISO/IEC 17799 – “Information Technology – Code of practice for information security management”
- BS7799 (British Standards Institute - subset)
- AS7799 (Australian standard for IT security management – subset)
- API 1164 – “SCADA Security”
- AGA 12 – “Cryptographic Protection for SCADA Communications General Recommendations”
- ISA SP99 – “Manufacturing and Control System Security Standard”
- API RP 70 Security of Offshore Oil and Natural Gas Operations
- NIST Standards:
  - NIST SP 800-12
  - NIST SP 800-14
  - NIST SP 800-26
- Applicable Internal BHP Billiton IT Standards also referenced

Standardized “Site Survey” used to Compare Facilities

- Created a common site survey form for assessing security posture at each facility
- Contacted local Operations and IT Systems “Custodians” to obtain answers to high-level questions
- Ranked all facilities in one large matrix with color code:
  - Green - adequate
  - Yellow - warning, security vulnerability with low risk
  - Red - warning, security vulnerability with high risk
- Allows prioritization for vulnerability mitigation
- Several strategic sites selected for full on-site assessment, and remaining sites will only receive the paper-based site survey

Remaining Phases in Roadmap

- The prioritized security vulnerabilities will require **Mitigation**
  - Existing technology will need to be re-configured
  - New technology may need to be installed
- The **Assessment** work is cyclical, since sites will need to be assessed after the mitigation work is complete to ensure high risks were removed
- The **Monitoring** phase includes:
  - Local NIDS and HIDS sensors
  - Centralized Outsourced SOC



Conclusion

- Creating a SCADA Security Roadmap is a key first step
- Defining Corporate SCADA Security Policies / Guidelines creates an internal standard for existing and new facilities
- When operations stretch across multiple country and continent boundaries, then all applicable International and Local Standards should be cross-referenced
- Resulting list contains only those standards sections that apply across the matrix, so compliance to one standard allows compliance to other related standards as well
- Partnering with a consulting firm that understands both SCADA Security Standards and Real Technical Solutions (paper and technology), allowed BHP Billiton to quickly create their Security Roadmap, assess risk, and prioritize mitigation strategies

Comments?

- Contact Information:
  - Jonathan Pollet, CAP, CISSP
  - Founder and VP of PlantData Technologies
  - Office: 1-877-302-DATA, ext 211
  - Cell: 1-281-748-6401
  - Email: jonathan.pollet@plantdata.com