Big Data and Cybersecurity in the Oil and Gas Industry
“Big data involves mashing up company data with public data to improve real-time reporting and predictive analysis.”

And Forensic analysis.

Jason Hiner, Editor in Chief of TechRepublic
Information Security Imperative

Confidentiality

Integrity

Availability

FISMA

COBIT

NERC

HIPAA

PCI
Remote Monitoring

- **Process Collaboration**
  - *Ensure operations are executed within Basis of Design limits*

- **Decision Support**
  - *Provide engineering support*

- **Real-Time Monitoring**
  - *Enhance early kick detection*

- **Forensic Capability**
  - *Aid root cause analysis*
Network Communication for Offshore Oil Drilling

- **Real Time Secure** Monitoring Lifecycle = $\sum ((\text{People} \times \text{Process} \times \text{Technology}) \rightarrow \text{Data at Rest}) + ((\text{People} \times \text{Process} \times \text{Technology}) \rightarrow \text{Data in Use}) + ((\text{People} \times \text{Process} \times \text{Technology}) \rightarrow \text{Data in Transit})$

- **Cost Benefit** = $(\text{Criteria} + \text{Design} + \text{Operation} + \text{Meeting Objectives}) / \text{Cost}$
Data Quality is Key

- Data sources
- Formats/standards
- Transmission methods
- Transmission frequency
- Authentication
- Validation
- Non-repudiation
RTM Big Data Reliability Context

Governance

Metrics

Controls

Confidentiality
Information kept private and secure

Integrity
Data not modified, deleted or added

Availability
Systems available to whom requires them
Continuous Monitoring Framework

Source: Continuous Monitoring and the Risk Management Framework at NIST

Development System → RTM Operations Center → BSEE Big Data Warehouse
Security Monitoring

- Policy Management
- Asset Management
- Data Management
- Vendor/Third Party Management
- Access Management
- Change Management
- Vulnerability Management
- Log Management
- Incident and Problem Management
- Business Continuity Management
- Risk Management
Parting thoughts

- **RTM information assurance is critical**
  - Controls necessary to maintain confidentiality, integrity, and availability of information supply chain

- **BSEE guidance must be pragmatic**
  - Specify data required
  - Prescribe control objectives for RTM data at rest, in use, in transit
  - Measure effectiveness of meeting controls

- **May want to establish Clearinghouse**
  - Manage big data
  - Maintain information security & privacy of proprietary data
  - Mitigate potential FOIA burden