# Cyber Security Solutions & Practices?
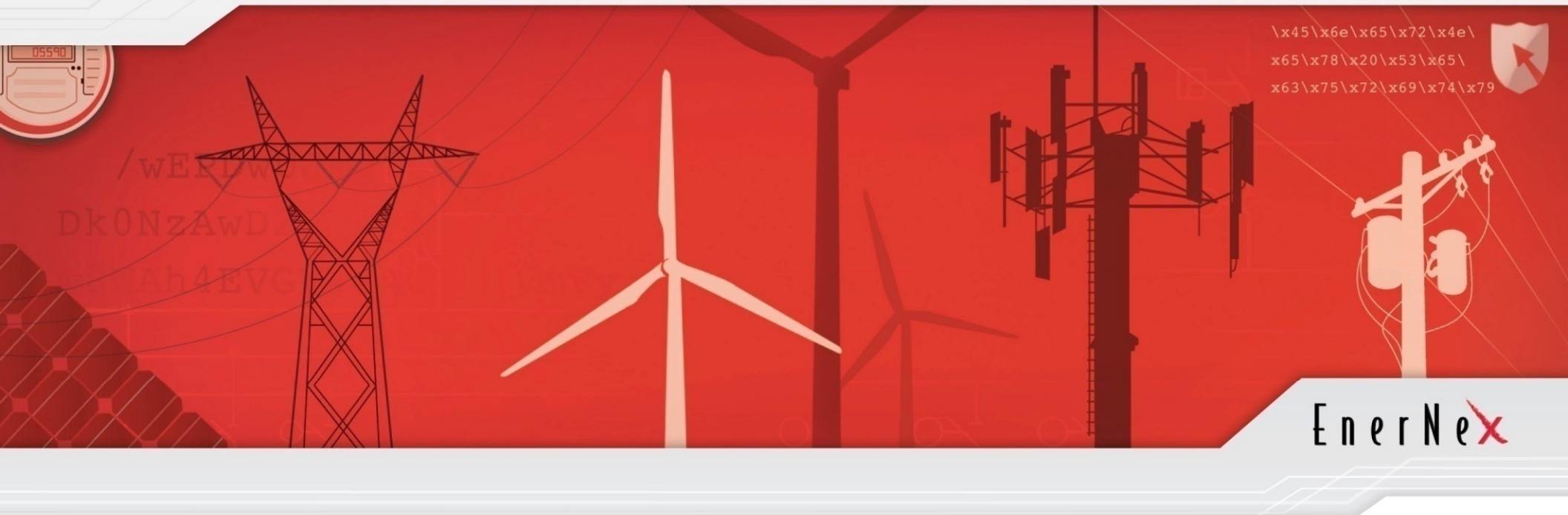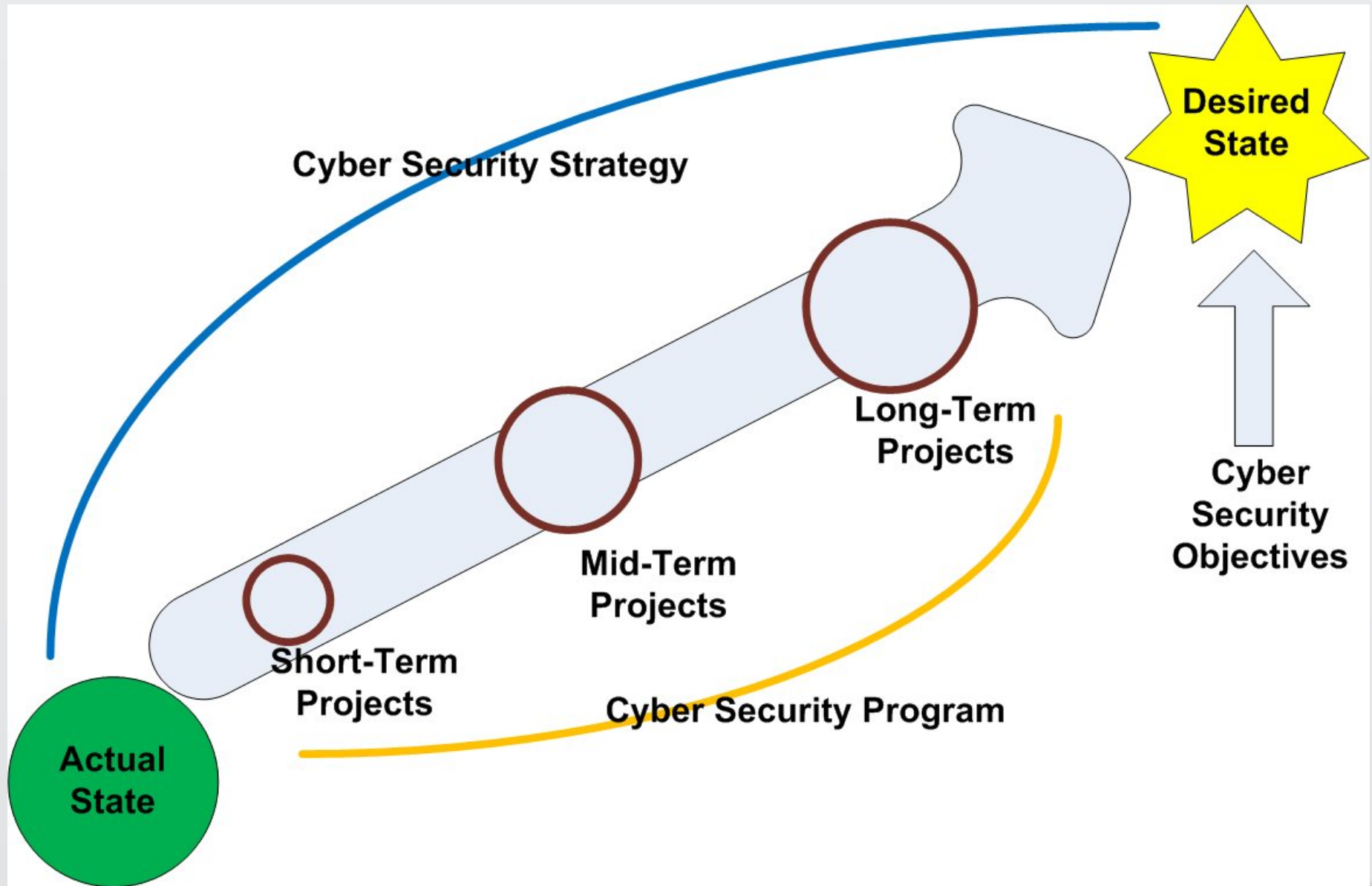
Presented By:

Sandy Bacik, Principal Consultant

EnerNex

# Cyber Security Strategy & Program

\x45\x6e\x65\x72\x4e\
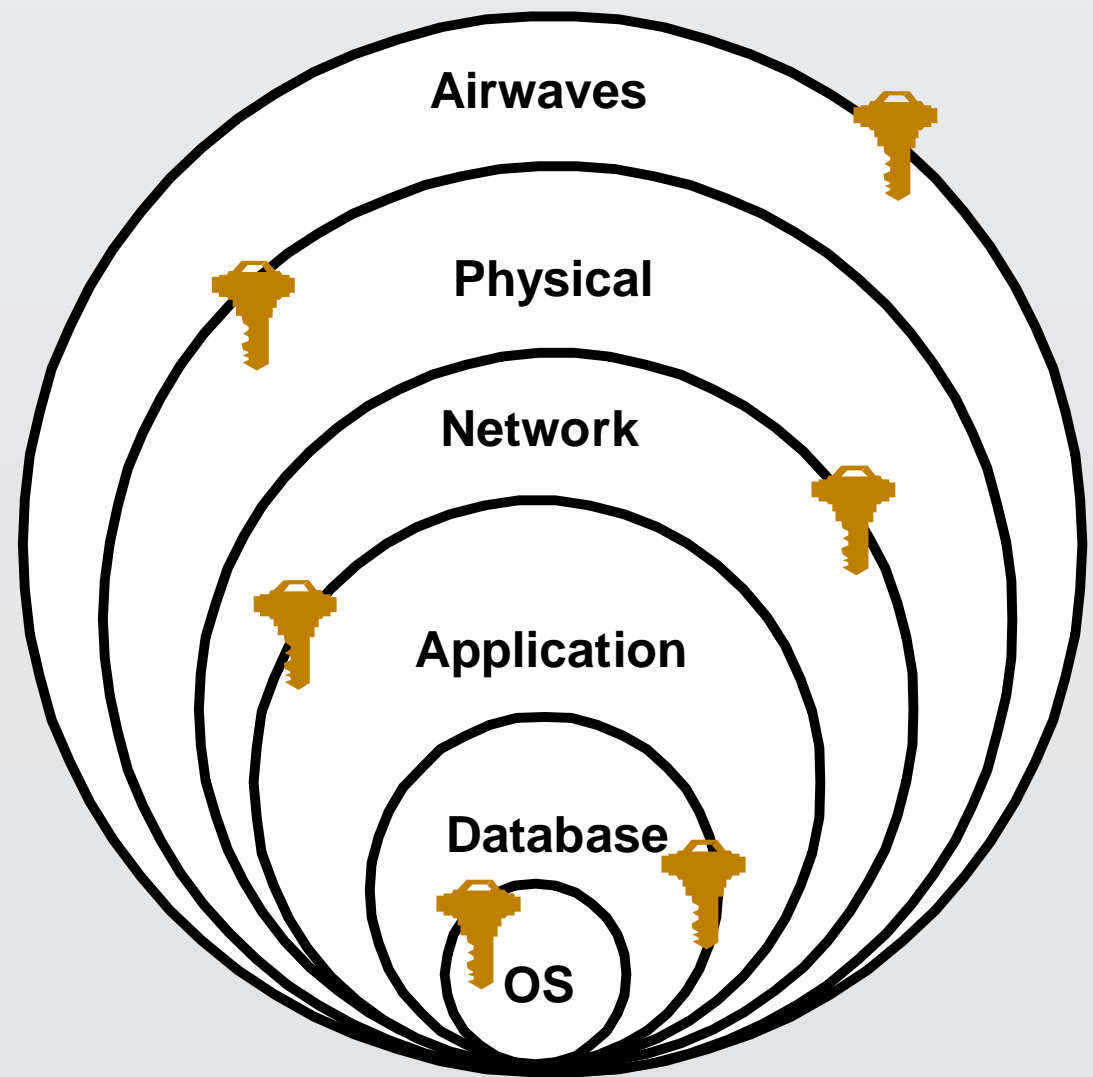x65\x78\x20\x53\x65\
x63\x75\x72\x69\x74\x79

# How Do We Govern Assets?

▶ Administrative and managerial measures

- Policies & procedures guide behavior
- Acceptable use
- Roles and responsibilities
- Serve business need
- Systems configured & maintained to policy specification
- ALL PEOPLE

▶ Physical

- Buildings, floors
- Locks, key cards, guards
- Hot, warm, off-site storage
- Desks, recycling & shred bins, dumpsters
- Cameras, access logs
- Background checks

▶ Technical measures

- Authentication
- Access control (segregation of duties)
- Audit
- Automated software
- Logging and monitoring

Grid-Interop 2011

# Asset Protection in Layers

▶ Need to establish depth-in-defense when implementing security

Airwaves

Physical

Network

Application

Database

OS

# Developing the Security Architecture

## STRATEGY
### Risk Management

Risk Treatment

Risk Analysis
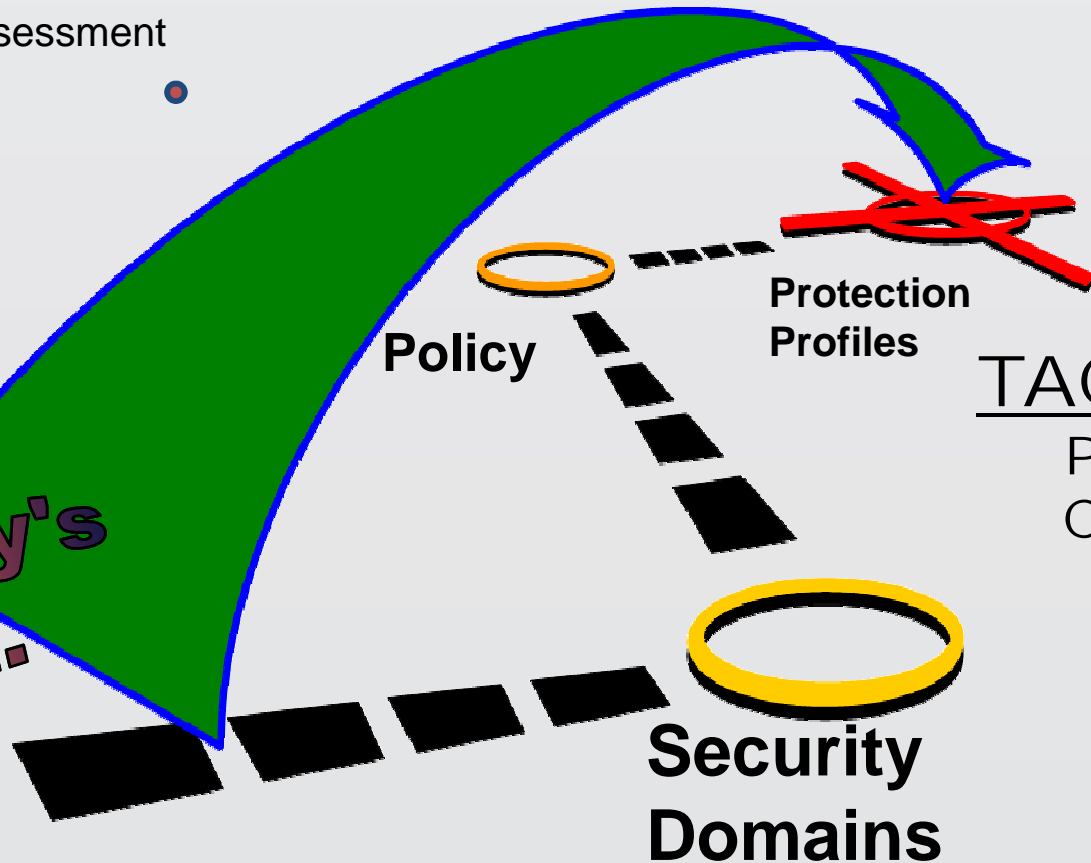
Cost / Benefit Analysis

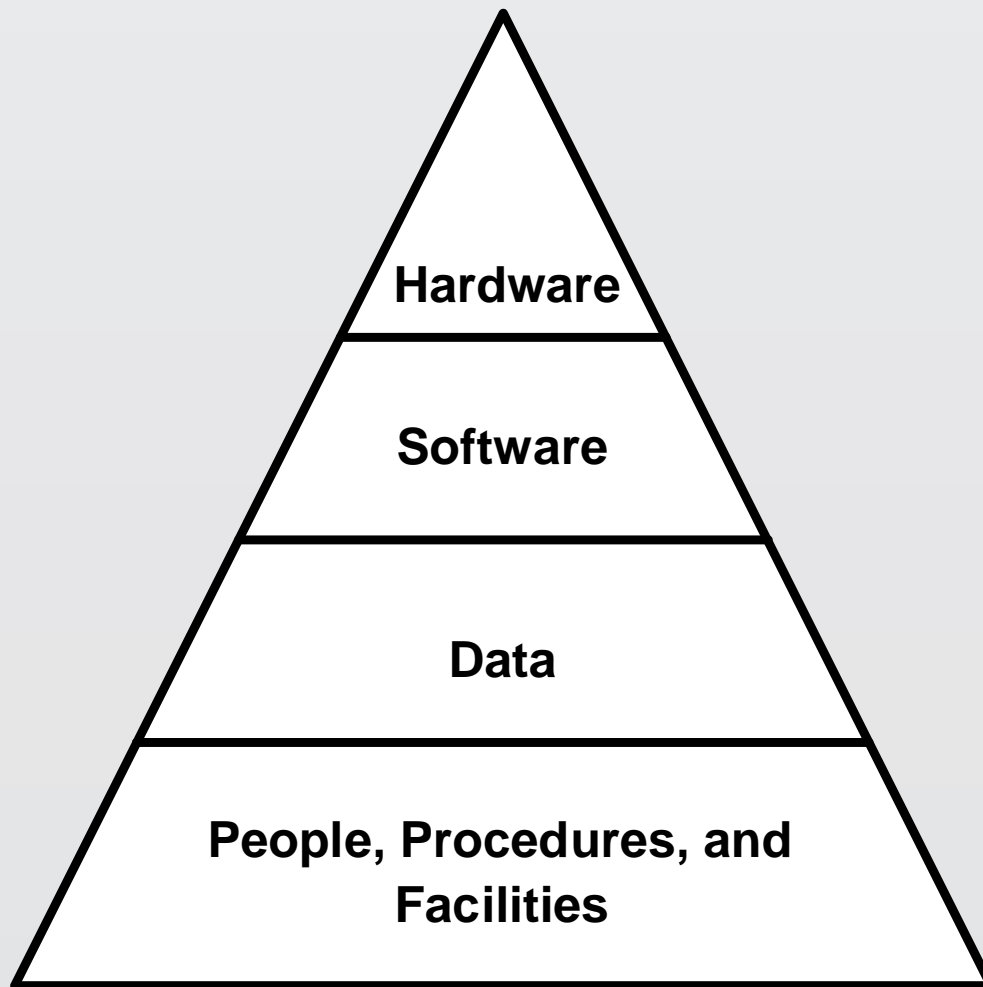Vulnerability Assessment

Threat Identification

Asset Identification

**Security? Somebody's got that... right?**

**Policy**

**Protection Profiles**

## TACTICS
### Process, Common Criteria

**Security Domains**

# Risk Triangle

Hardware

Software
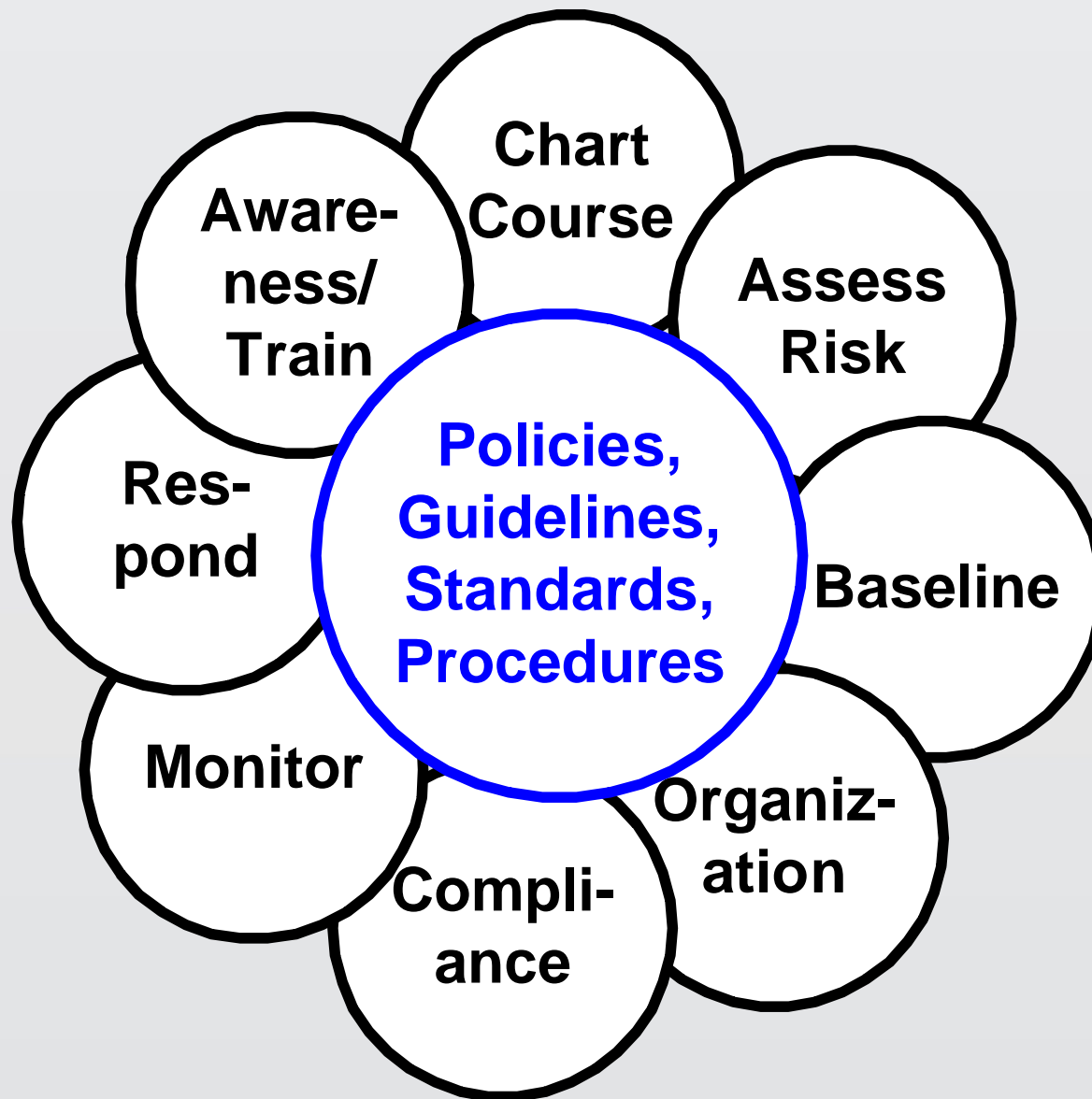
Data

People, Procedures, and Facilities

Hardware and software is replaceable, it is not customized

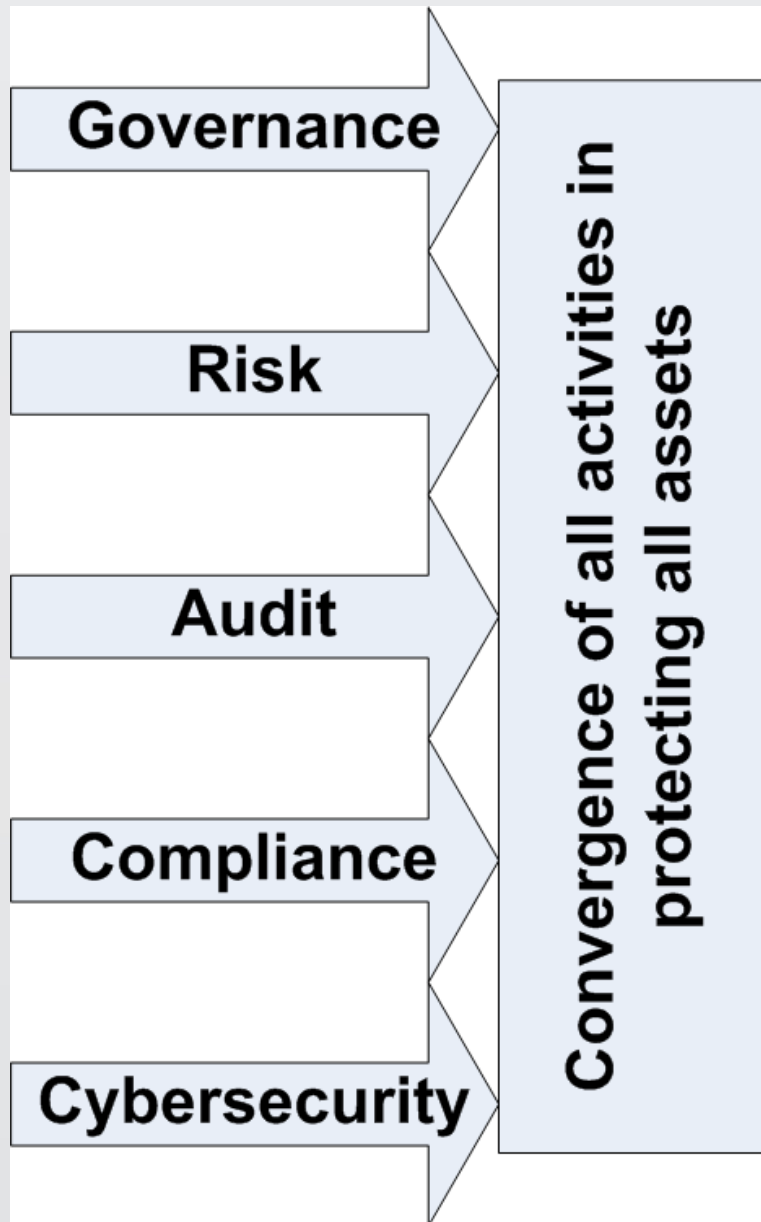Data risk is larger, because it takes much to recreate it should something happen

People are sometimes a wildcard when dealing with assets

# Continuous Process



- Chart Course
- Aware-ness/Train
- Assess Risk
- Res-pond
- **Policies, Guidelines, Standards, Procedures**
- Baseline
- Monitor
- Organiz-ation
- Compli-ance

Reference: Building an Effective Information Security Policy Architecture, by Sandy Bacik, Page16.

Grid-Interop 2011

# Convergence



Governance → Risk → Audit → Compliance → Cybersecurity → **Convergence of all activities in protecting all assets**

Think about all areas, including the business processes, when developing asset protection.

Saves time in the future.

# Cyber Security Strategy Basic Foundation

1. Strategic Alignment
2. Executive Management Support
3. Regulatory Requirements
4. Cyber Security Strategy Framework
5. Current State
6. Desired State
7. Cyber Security Program framework
8. Create the Cyber Security Program
9. Establish Key Performance Indicators
10. Do – Check – Act

# EnerNex Cyber Security Offerings

▶ Security Architecture and Policy Development

▶ Utility Automation Security

▶ NERC-CIP

▶ Hardware Embedded Security

▶ Security & Penetration Testing

▶ Vulnerability Analysis

▶ Risk Assessments

▶ Security Audit Development

▶ Regulatory Compliance

▶ Security Training



**STRATEGY** Risk Management

Cost / Benefit Analysis
Risk Treatment
Risk Analysis
Vulnerability Evaluation
Threat Evaluation
Asset Evaluation

Policy
SECURITY ARCHITECTURE
Security Domains

SECURITY?!

▶ Clients: Consumers Energy, U.S Department of Energy, Duke Energy, Florida Power & Light (FPL), Southern California Edison (SCE), Tennessee Valley Authority (TVA), TXU Energy

Grid-Interop 2011
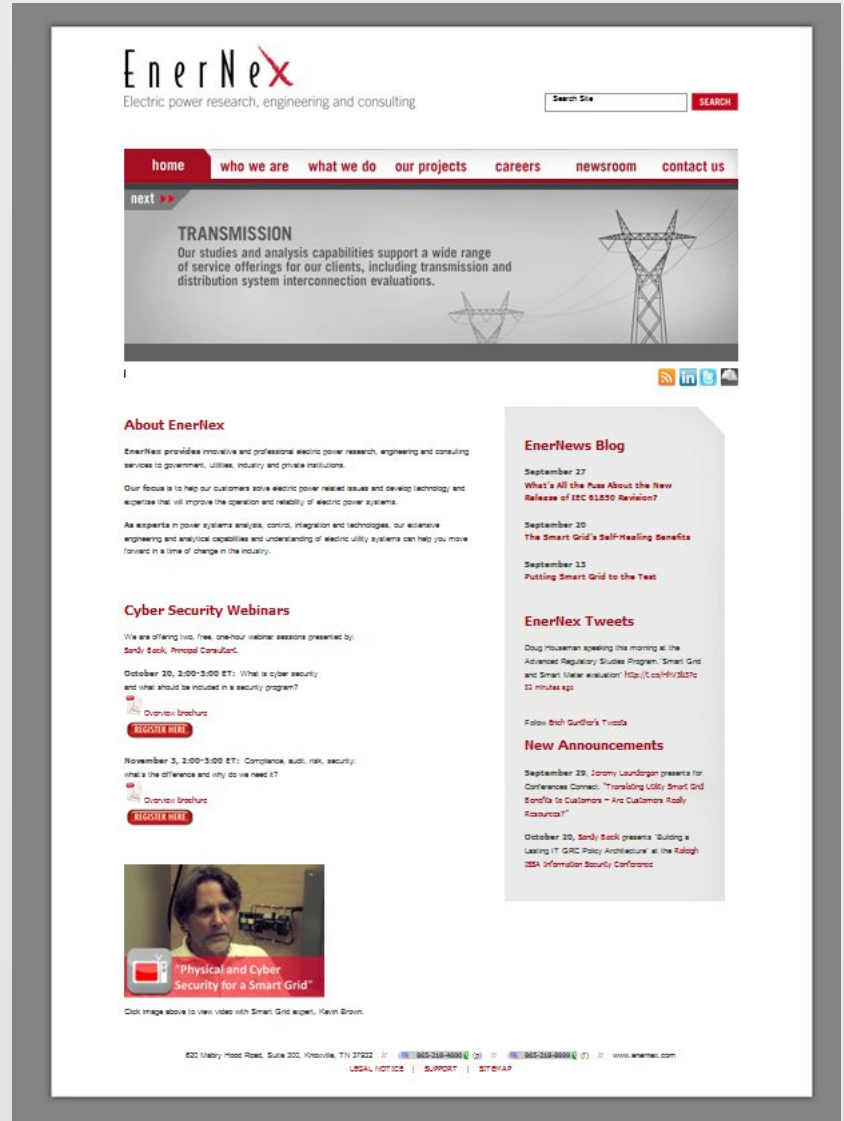
# Thank you for attending

▶ Contact me:  [sandy.bacik@enernex.com](mailto:sandy.bacik@enernex.com)

▶ Visit us on the web:  [www.enernex.com](http://www.enernex.com)

Follow us on Twitter @ EnerNex

Connect with us on LinkedIn

Subscribe to the EnerNex blog

Grid-Interop 2011