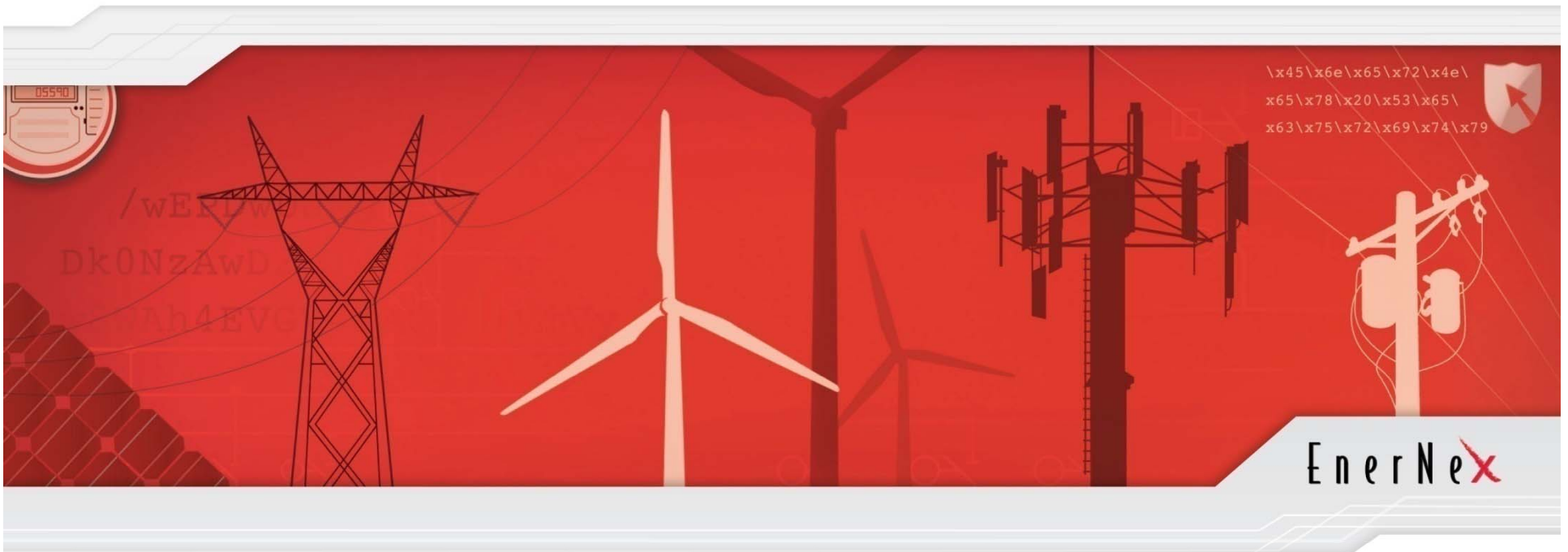


What is Cybersecurity and What Should be Included in a Security Program?

Presented By:

Sandy Bacik, Principal Consultant





Agenda

- ▶ Defining security and safety
- ▶ What does security include?
- ▶ Overview of what is included in a security program versus an information security program
- ▶ Things to consider when building a security program



Information Warfare

“There’s a war out there old friend – A world war – and it’s not about who’s got the most bullets; it’s about who controls the information. What we see and hear, how we work, what we think, it’s all about the information!”

- Ben Kingsley, Sneakers, 1992

The Enterprise vs. Professional Bad Guys

▶ Enterprise

- Laws, Regulations
- Limited / Tight budgets
- Limited staff
- 9-5, M-F, time off
- Many times, unappreciated
- Responsible to protect against unlimited attack vectors

▶ Bad guys

- No rules
- Well funded
- Active 24 / 7/ 365
- Mostly, motivated “\$\$\$”
- Take the path of least resistance
- Bored and looking for a challenge

The banner features a grayscale background with various energy-related icons: a digital meter on the left, a high-voltage power transmission tower in the center, and a wind turbine on the right. In the top right corner, there is a small shield icon and a block of hex code: \x45\x6e\x65\x72\x4e\x65\x78\x20\x53\x65\x63\x75\x72\x69\x74\x79. The main title 'Energy Sector Industry Challenges' is written in a large, bold, black sans-serif font across the middle of the banner.

Energy Sector Industry Challenges

- ▶ Security is more **IMPORTANT** than ever before as control systems are evolving
 - Increasing use of varied communication methods
 - Lower installation costs
 - Additional connections to external systems
 - Supports changing operational and business needs
 - New and emerging regulatory requirements
- ▶ Security is more **COMPLICATED** than before
 - Utilities are faced with limited security expertise
 - It shouldn't take a security expert to configure a device properly!
 - Vendors need alternatives to proprietary solutions
 - Utilities and Vendors need a straight forward method to communicate user needs, product features, and configuration parameters relating to cyber security functions

A Systems View of the Modern Grid

Key Success Factors

- Reliable
- Security
- Economics
- Quality
- Efficiency/Environmental Quality
- Safety

Metrics

- Congestion Costs
- Massive Blackout Probability
- Restoration Time
- Peak to Average Load Ratio
- Capacity Utilization

Performance

- Emergency Response
- Restoration
- Routine Operations
- Optimization of Assets
- Systems Planning

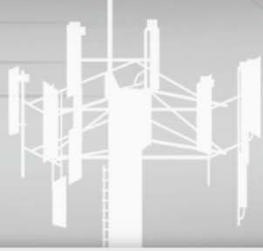
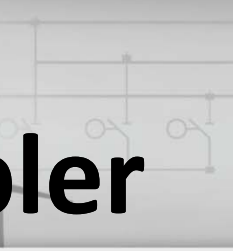
Characteristics

- Self-healing
- Integrated at all levels
- Distributed
- Predictive
- Empowers/Incorporates Consumer
- Tolerant of Security Attack
- Power Quality for 21st Century
- Wide Variety of Generation Options
- Enables Electricity Markets

Key Technologies

- Integrated Communications
- Advanced Control Methodologies
- Sensing, Metering, and Measurement
- Advanced Grid Components
- Decision Support & Human Interfaces

Source: Overview of the Modern Grid Initiative, S Pullins, MGI Team, NETL, DOE



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



Security as Enabler



Security and Safety – the same thing?

Safety

- ▶ Freedom from danger, risk, or injury.
- ▶ A device designed to prevent accidents
- ▶ The condition of being safe from undergoing or causing hurt, injury, or loss
- ▶ A device designed to prevent inadvertent or hazardous operation

Security

- ▶ Freedom from risk or danger
- ▶ Freedom from doubt, anxiety, or fear; confidence.
- ▶ Something that gives or assures safety, as:
 - A group or department of private guards
 - Measures adopted to prevent espionage, sabotage, or attack.

Security and Cybersecurity

Security

- ▶ Freedom from risk or danger
- ▶ Freedom from doubt, anxiety, or fear; confidence.
- ▶ Something that gives or assures safety, as:
 - A group or department of private guards
 - Measures adopted to prevent espionage, sabotage, or attack.

Cybersecurity

- ▶ A measure of system's ability to resist unauthorized attempts at usage or behavior modification, while still providing service to legitimate users.
- ▶ The protection of data and systems
- ▶ Actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted (DoD)



Parkerian Hexad

- ▶ Six fundamental, atomic, non-overlapping attributes of information that are protected by information security measures
- ▶ Defined by Donn B. Parker in 2002, renowned security consultant and writer, they are
 - Confidentiality
 - Possession / Control
 - Integrity
 - Authenticity
 - Availability
 - Utility



Cybersecurity – IT versus Control Systems

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



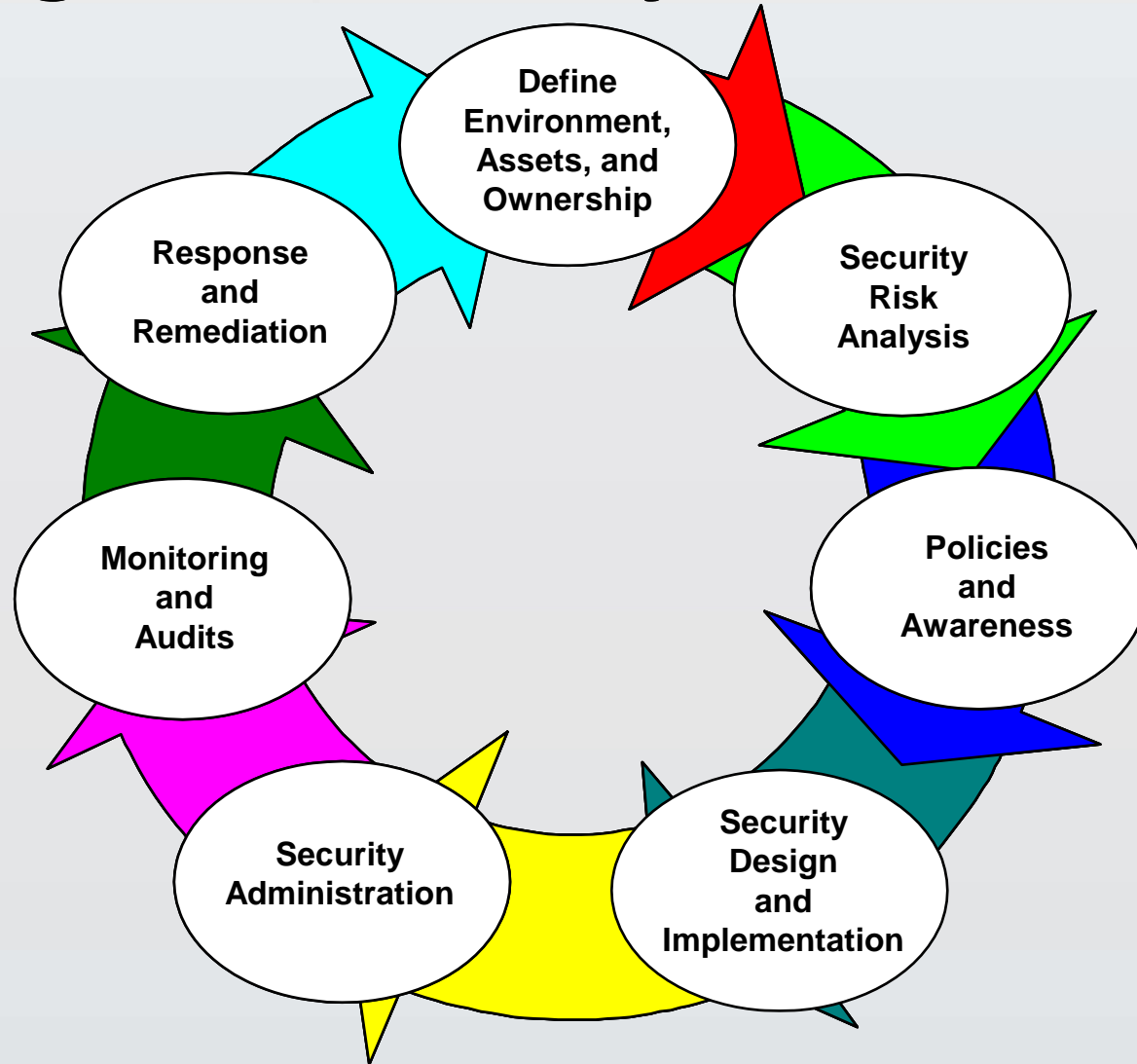
- ▶ How we secure IT systems is not the way we can secure control systems
 - Shifting and combining the analog / electro-mechanical and digital environments
- ▶ IT focuses on confidentiality and integrity
 - Many cybersecurity issues
 - Almost a disposable environment
- ▶ Control systems focus on integrity and availability
 - Not many cybersecurity issues
 - Equipment lifecycle a few months to a few years



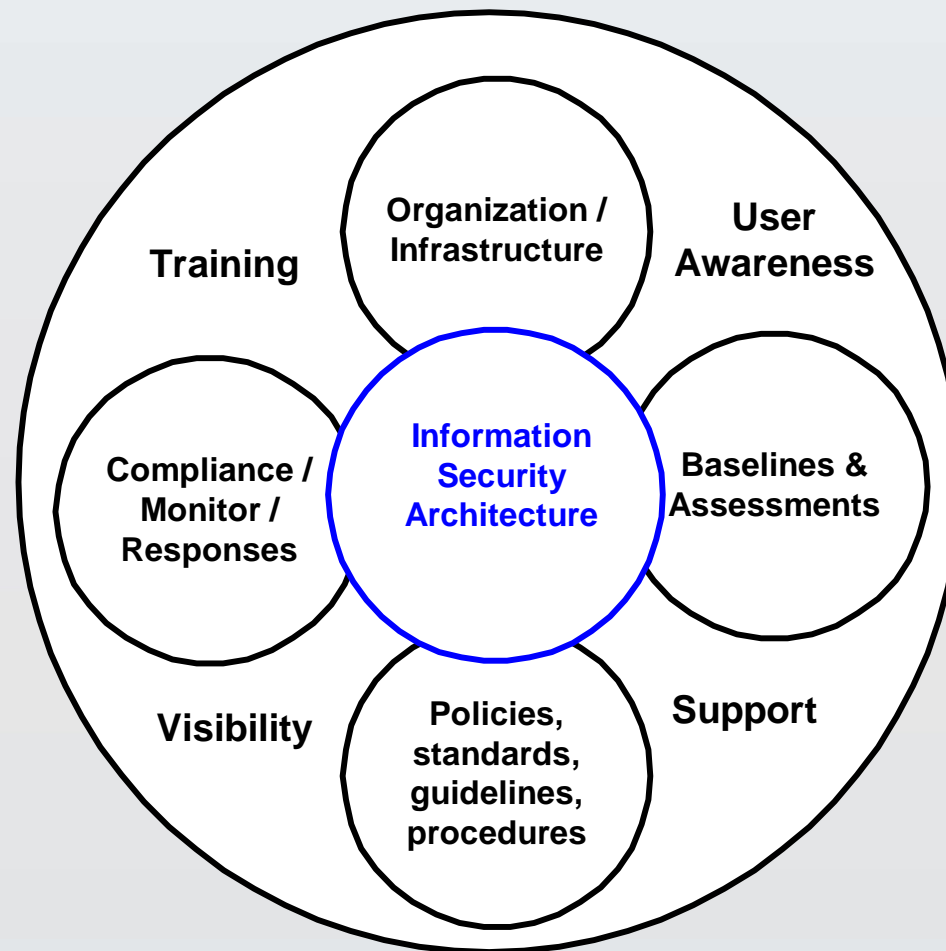
We Know

- ▶ If we can persuade you to run something, it's not your machine anymore
- ▶ If someone can alter your OS, it's not your machine anymore
- ▶ If someone can gain physical access, it's not your area anymore
- ▶ If someone can upload to your machine or website, it's not yours anymore
- ▶ Weak passwords ruin strong security
- ▶ An environment as secure as personnel are trustworthy
- ▶ Encryption is only as secure as the decryption key
- ▶ Out-of-date virus scanners are only a bit better than no virus scanner
- ▶ Anonymity is not practical
- ▶ Technology is not a panacea

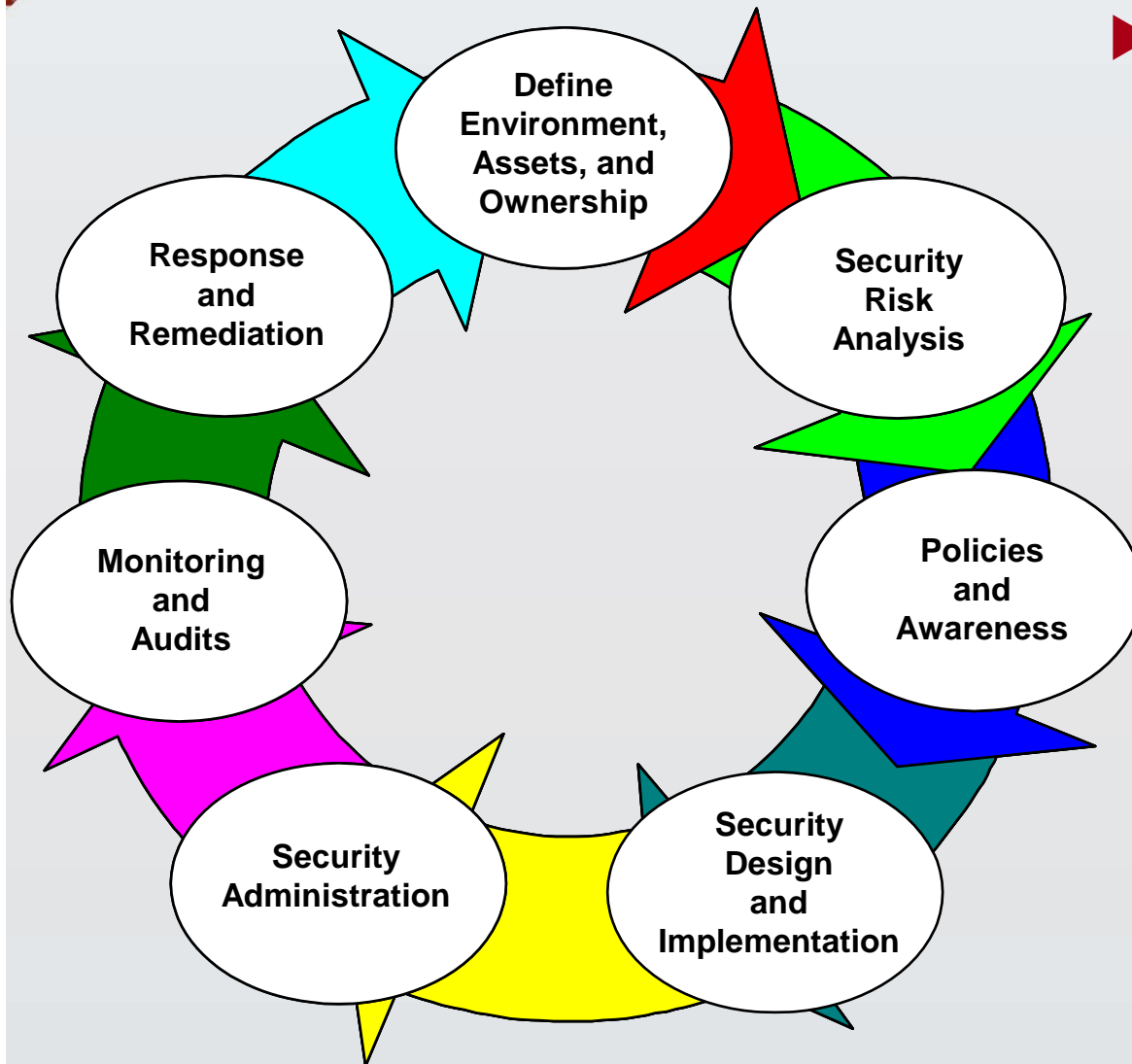
Information Security Management Lifecycle



What an Information Security Program Contains



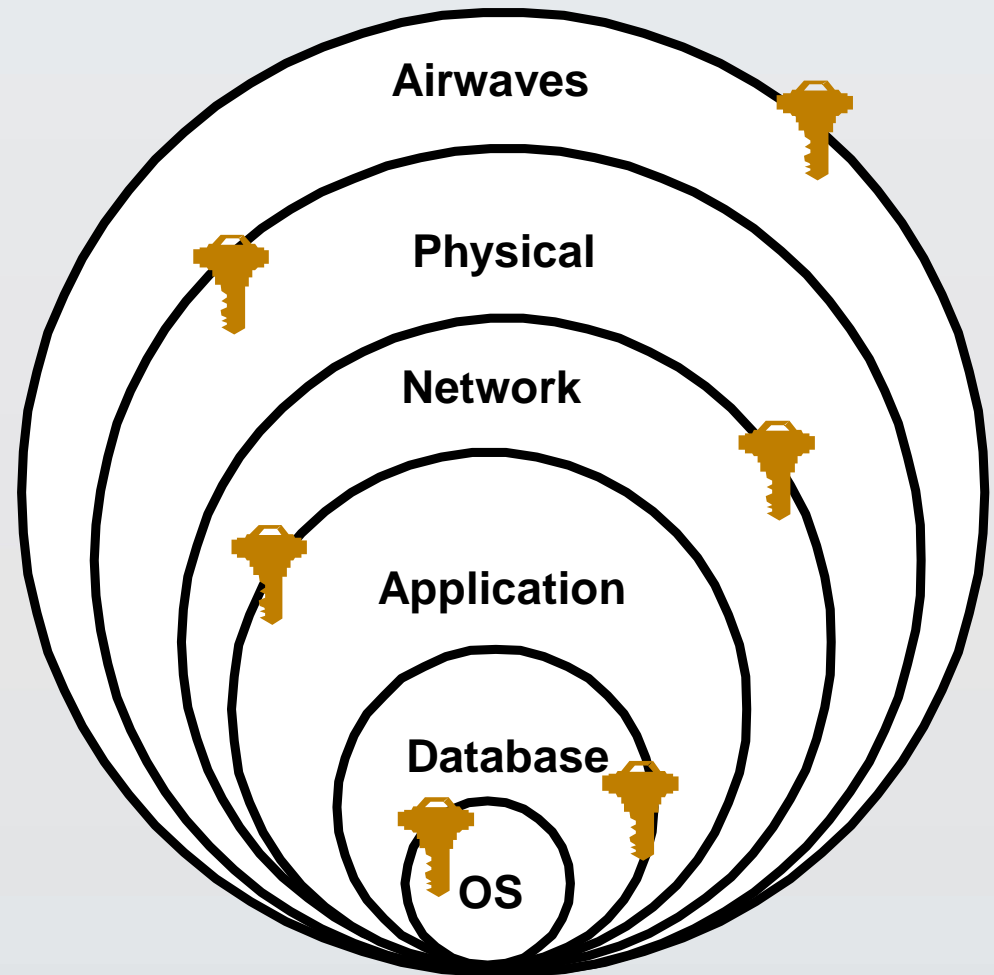
Security Management Lifecycle



- ▶ Need to add
 - Personnel Security
 - Facilities / Property / Restricted areas
 - Physical Security Equipment
 - Identification cards / Badges
 - Guards

Asset Protection in Layers

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





Physical Security Thoughts

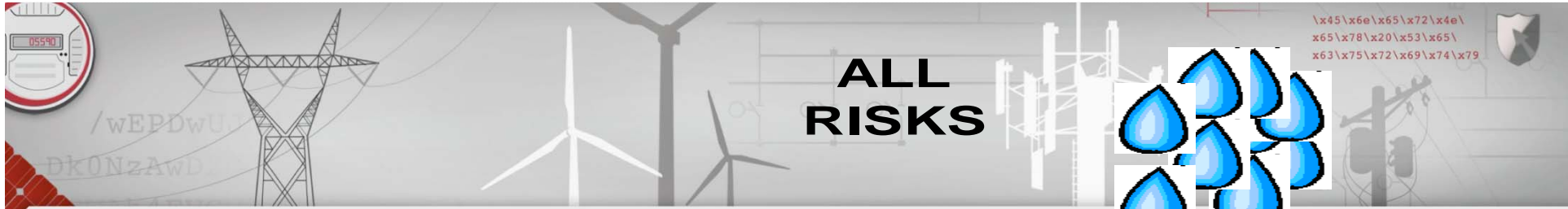
\x45\x6e\x65\x72\x4e\
x65\x78\x20\x53\x65\
x63\x75\x72\x69\x74\x79

- ▶ **Deterrence** provides countermeasures and controls to defend against attacks on the assets being protected
- ▶ **Detection** monitors for potential breakdowns in protective mechanisms that could result in security breaches
- ▶ **Delay** is a necessary measure if there is a breach, to slow down the intruders long enough to allow a security team to apprehend them before they achieve their objective
- ▶ **Response**, which requires human involvement, covers procedures and actions for assessing the situation and responding to a breach
- ▶ **Recovery** is your plan to continue business and operations as normally as possible following an incident
- ▶ **Re-evaluation** is critical. You must constantly keep your physical security under review and keep re-visiting your original assessment and objectives



Principles and Strategies

- ▶ Security as a holistic approach
- ▶ Security as a public / private collaborative (nationally / globally)
- ▶ Build security into the business requirements and processes
- ▶ Standard set of security standards, practices, and requirements
- ▶ Standardized testing (conformity / security)
- ▶ Awareness to the enterprise, third parties and customers, including privacy
- ▶ Not reinventing the wheel for all the above



**ALL
RISKS**



POLICY



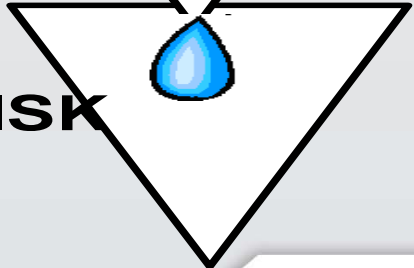
**GUIDELINES,
STANDARDS, &
PROCEDURES**



TECHNOLOGY



RESIDUAL RISK



Need to establish a risk baseline before you start selecting and implementing security requirements

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



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

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

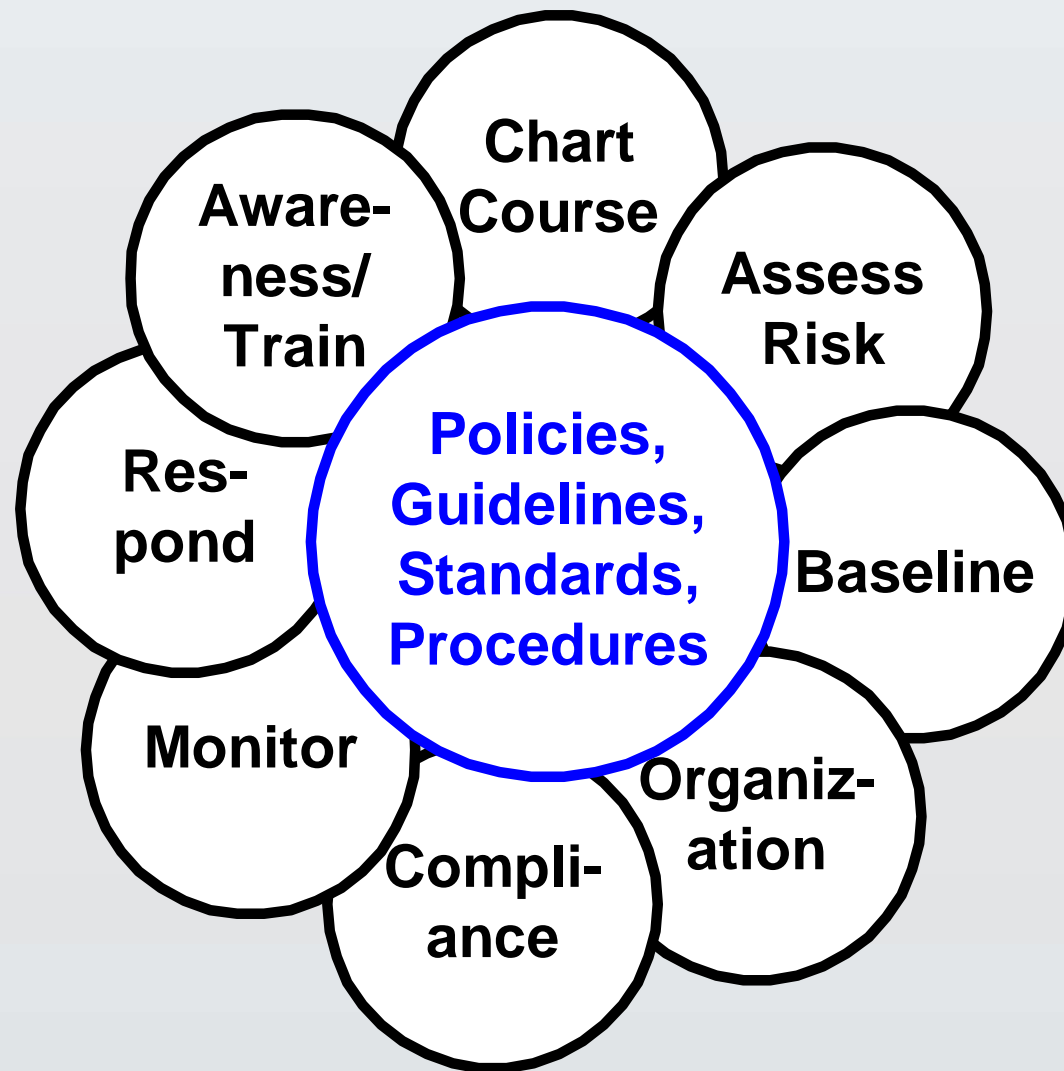
▶ Physical

- 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

Continuous Process



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



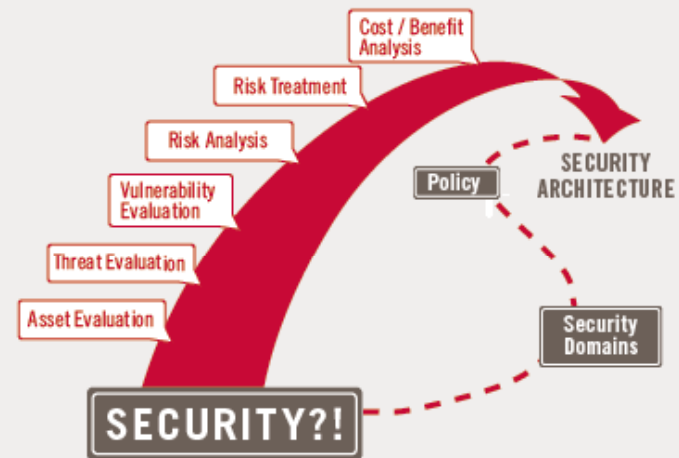
What you need to consider?

- ▶ Continually evaluating risk
- ▶ Continually reviewing, evaluating, testing controls (and compensating controls)
- ▶ Communication with the business, executives, and operations
- ▶ What already exists?
- ▶ Culture

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



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

Thank you for attending

▶ Contact me: sandy.bacik@enernex.com

▶ Visit us on the web: www.enernex.com



Follow us on Twitter @ EnerNex



Connect with us on LinkedIn



Subscribe to the EnerNex blog

EnerNex
Electric power research, engineering and consulting

home | who we are | what we do | our projects | careers | newsroom | contact us

next >>

TRANSMISSION

Our studies and analysis capabilities support a wide range of service offerings for our clients, including transmission and distribution system interconnection evaluations.

About EnerNex

EnerNex provides innovative and professional electric power research, engineering and consulting services to government, utilities, industry and private institutions.

Our focus is to help our customers solve electric power related issues and develop technology and expertise that will improve the operation and reliability of electric power systems.

As experts in power systems analysis, control, integration and technologies, our extensive engineering and analytical capabilities and understanding of electric utility systems can help you move forward in a time of change in the industry.

EnerNews Blog

September 27
What's All the Fuss About the New Release of IEEE 61850 Revision?

September 20
The Smart Grid's Self-Healing Benefits

September 13
Putting Smart Grid to the Test

EnerNex Tweets

Doug Hausman speaking this morning at the Advanced Regulatory Studies Program: Smart Grid and Smart Meter evaluation. <http://bit.ly/1257t2e> @EnerNex

Follow Bob Gardner's Tweets

New Announcements

September 19, Jeremy Lundgren presents for Conference Connect: "Translating Utility Smart Grid SandUs to Customers - Are Customers Really Ready?"

October 20, Sandy Bacik presents "Building a Learning IT Data Policy Architecture at the Raleigh 2011 Information Security Conference"

Cyber Security Webinars

We are offering two, free, one-hour webinar sessions presented by: **Sandy Bacik, Principal Consultant.**

October 20, 2:00-3:00 ET: What is cyber security and what should be included in a security program?

REGISTER HERE

November 3, 2:00-3:00 ET: Compliance, audit, risk, security: what's the difference and why do we need it?

REGISTER HERE

"Physical and Cyber Security for a Smart Grid"

Click image above to view video with Smart Grid expert, Kevin Brown.

620 Liberty Road, Suite 200, Knoxville, TN 37922 | 865-218-8800 (a) | 865-218-8800 (r) | www.enernex.com
LEGAL NOTICE | SUPPORT | SITE MAP