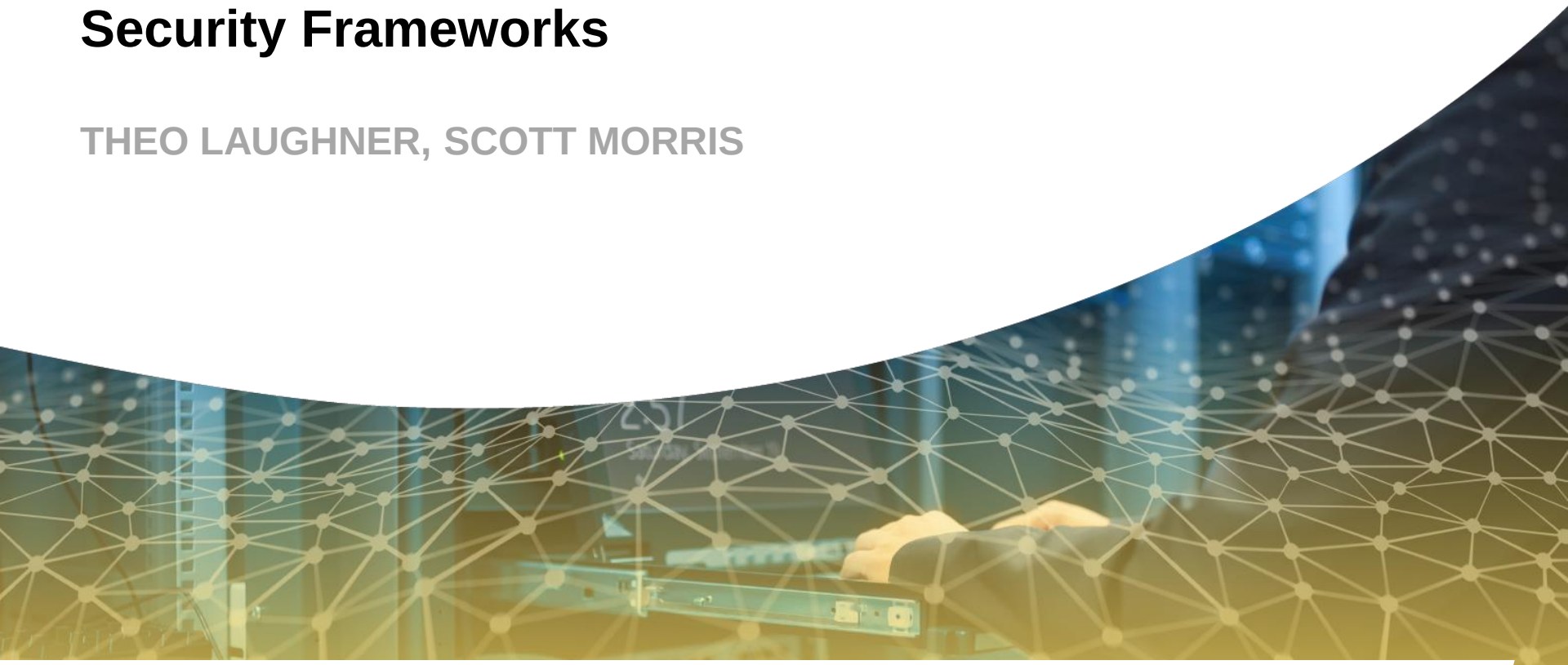
POWER GRID-RX INC
PRESCRIPTIONS FOR THE POWER GRID IN THE DIGITAL AGE

ALCHEMY GLOBAL NETWORKS

Introduction to Cyber Security and Cyber Security Frameworks

THEO LAUGHNER, SCOTT MORRIS



INTRODUCTION

INTRODUCTION

Threat

An expression of intention to ***inflict evil, injury, or damage.***

INTRODUCTION

Security

Measures taken to guard against ***espionage, crime, attack, or escape.***

INTRODUCTION

Risk

The possibility that something bad or unpleasant will happen.

Typical Threats

Animals

People

INTRODUCTION

Typical Mitigation

Fences

Personnel

Cameras

Lights

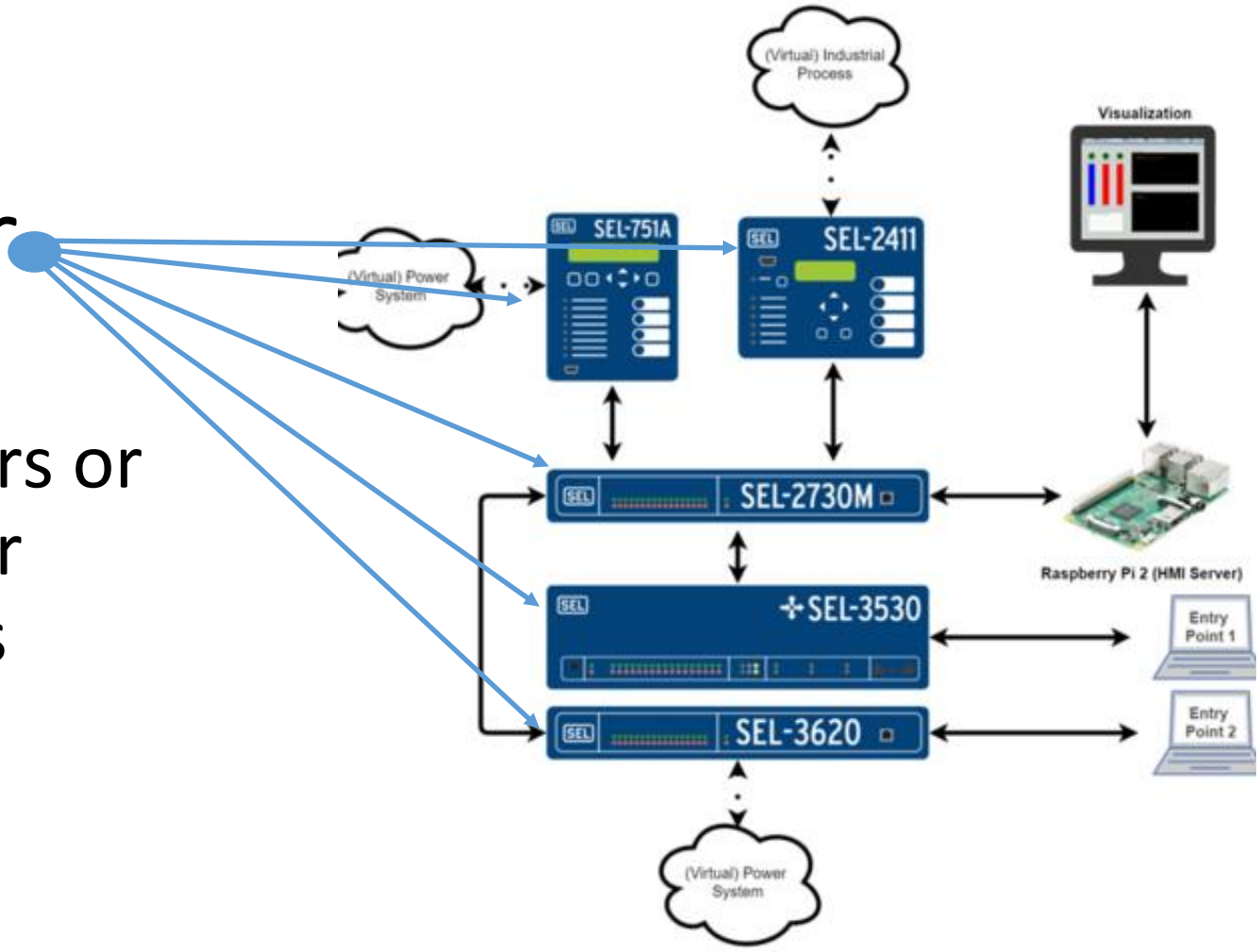
Cannons!

CYBER…

CYBER

Cyber

Involving computers or computer networks



Cyber Threats

A possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.

Hacker

a person who illegally gains access to and sometimes tampers with information in a computer system

Security

Measures taken to guard against ***espionage, crime, attack, or escape.***

Cyber Security

The protection of internet-connected systems, including hardware, software and data, from cyber threats

Substations Evolved

SUBSTATION EVOLUTION

Grid

Meters Read By People
Electromechanical Relays
Manned Substations
Routine Inspections

Smart Grid

Automatic Meter Reading
Microprocessor Relays
Unmanned Substations (SCADA)
Online Inspections

DISCONNECTED → **CONNECTED**

Regulation

REGULATION

- 2014 EXECUTIVE ORDER 13636

  Mandates improvements to cybersecurity architectures for critical infrastructure programs.

REGULATION

- NERC CIP

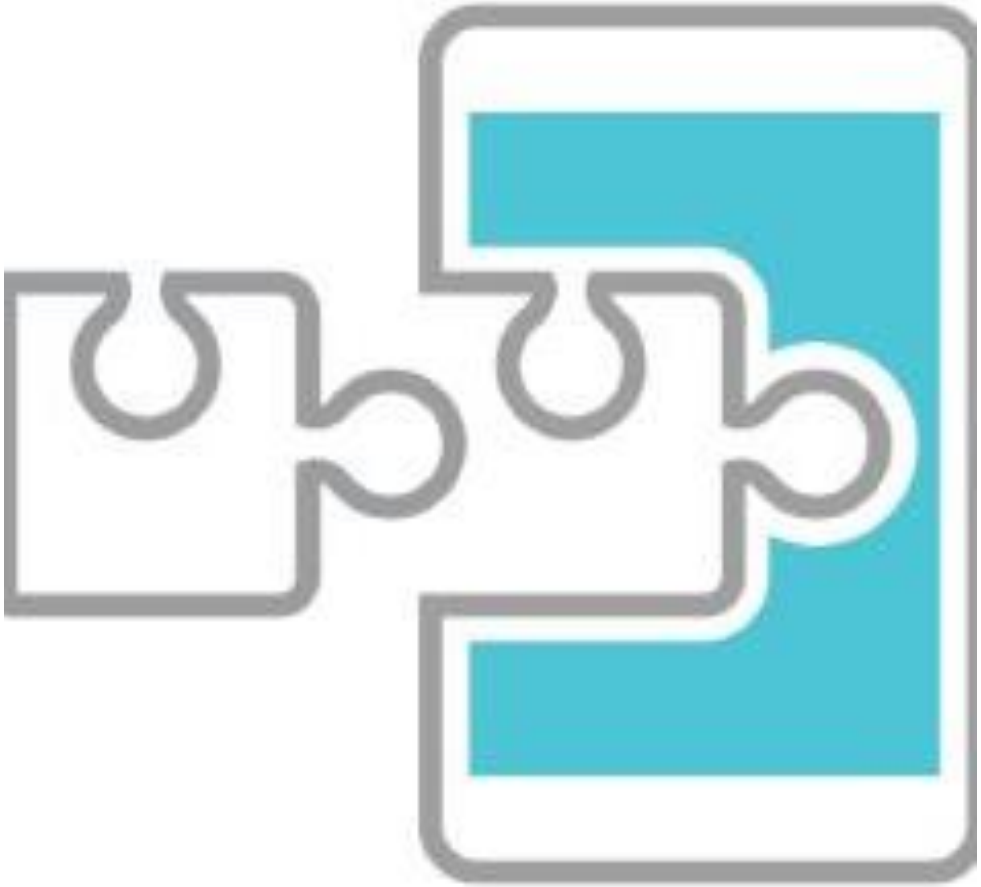
  A set of regulations mandating cyber protection for critical electric infrastructure.

Cyber Frameworks

CYBER FRAMEWORKS

FRAME WORK

A basic conceptual structure



CYBER FRAMEWORKS

- Cybersecurity Framework

  Provide guidance on managing risk to threats from cyber attacks. Often include ***standards, guidelines, and best practices*** when developing elements of a cybersecurity program.

CYBER FRAMEWORKS

Example Frameworks

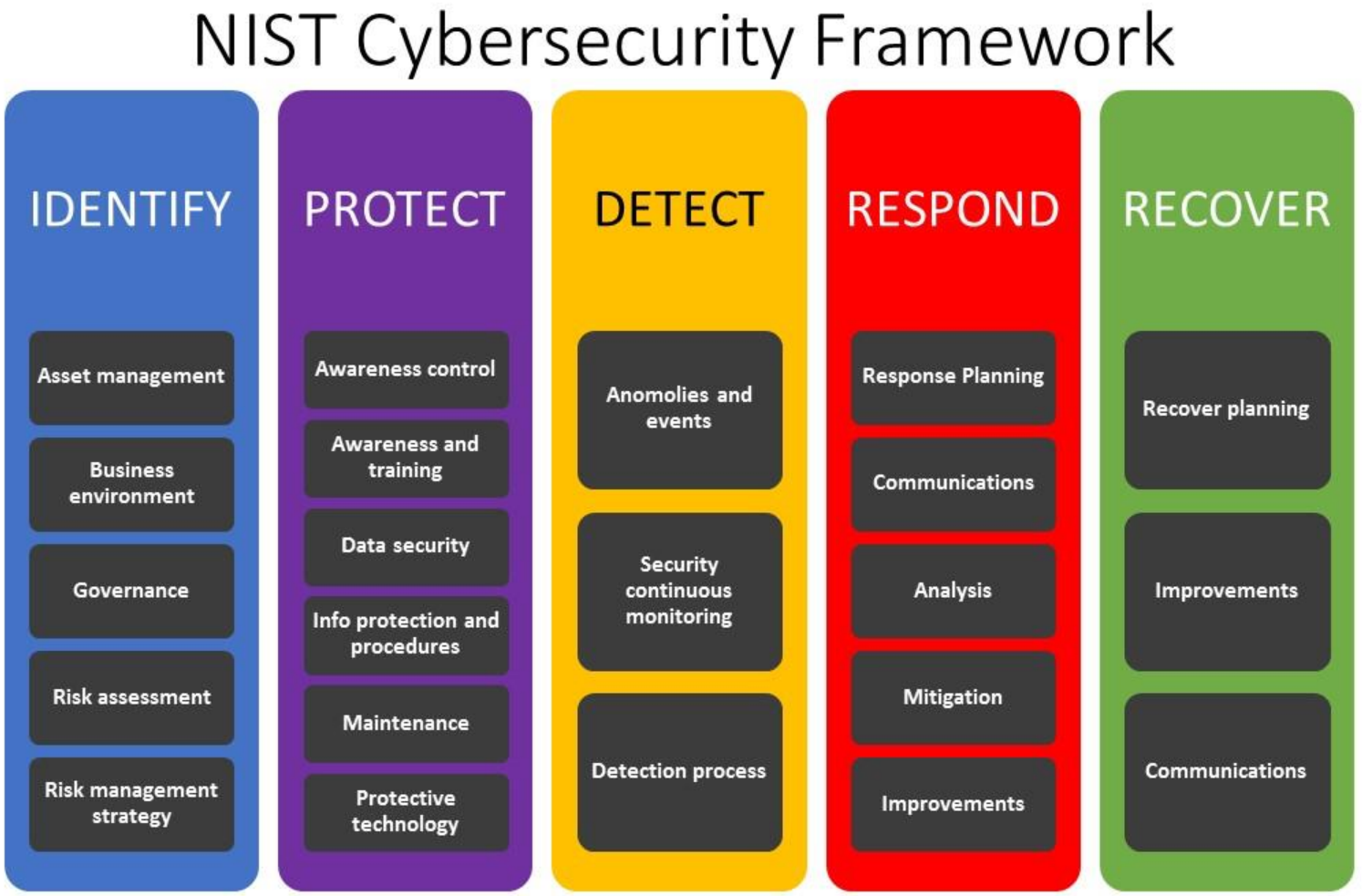
- PCI DSS
- ISO 27001/27002
- CIS
- NIST Framework

CYBER FRAMEWORKS

Consequences

- Fines for non-compliance
- Data Breach
- Equipment Failure

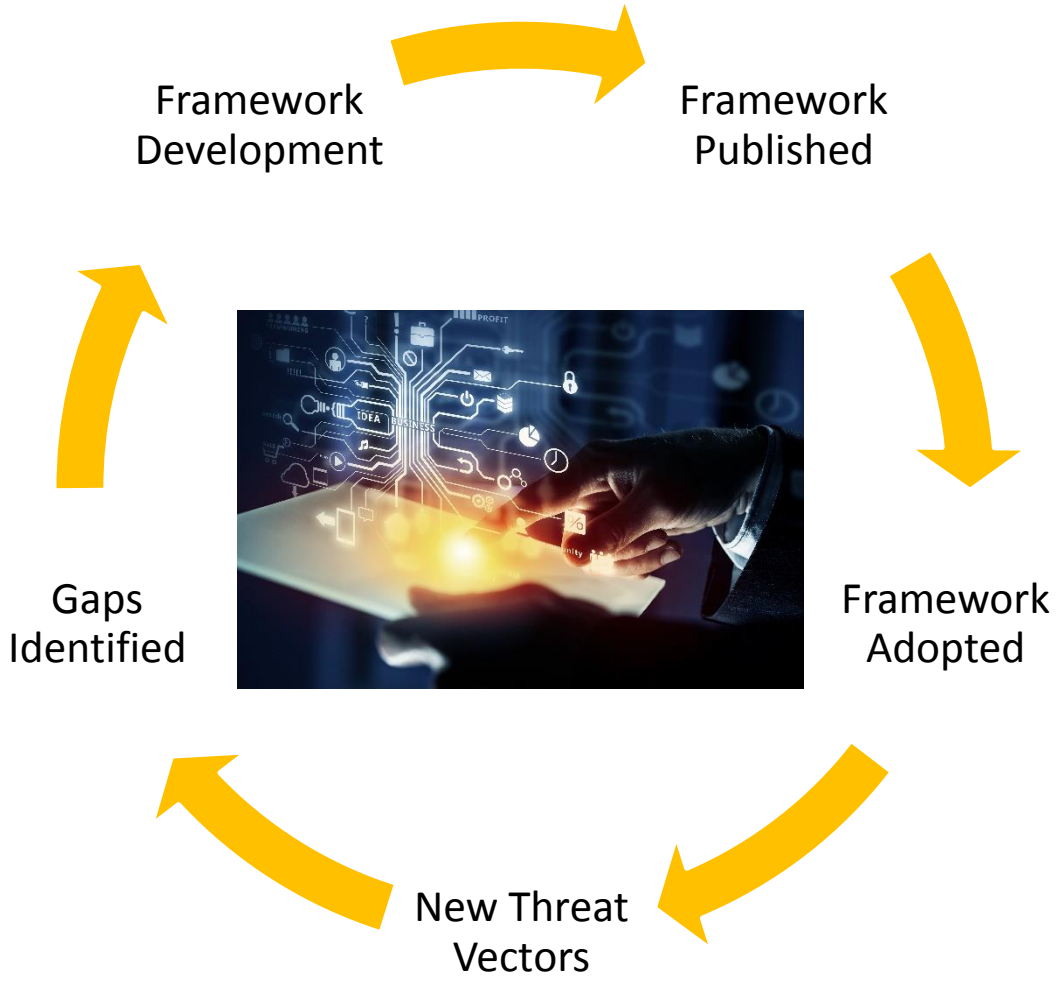
CYBER FRAMEWORKS



CYBER FRAMEWORKS

Category	Subcategory	Informative References
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	- **CCS CSC** 1 - **COBIT 5** BAI09.01, BAI09.02 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISA 62443-3-3:2013** SR 7.8 - **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 - **NIST SP 800-53 Rev. 4** CM-8
	ID.AM-2: Software platforms and applications within the organization are inventoried	- **CCS CSC** 2 - **COBIT 5** BAI09.01, BAI09.02, BAI09.05 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISA 62443-3-3:2013** SR 7.8 - **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 - **NIST SP 800-53 Rev. 4** CM-8
	ID.AM-3: Organizational communication and data flows are mapped	- **CCS CSC** 1 - **COBIT 5** DSS05.02 - **ISA 62443-2-1:2009** 4.2.3.4 - **ISO/IEC 27001:2013** A.13.2.1 - **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
	ID.AM-4: External information systems are catalogued	- **COBIT 5** APO02.02 - **ISO/IEC 27001:2013** A.11.2.6 - **NIST SP 800-53 Rev. 4** AC-20, SA-9
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	- **COBIT 5** APO03.03, APO03.04, BAI09.02 - **ISA 62443-2-1:2009** 4.2.3.6 - **ISO/IEC 27001:2013** A.8.2.1 - **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	- **COBIT 5** APO01.02, DSS06.03 - **ISA 62443-2-1:2009** 4.3.2.3.3 - **ISO/IEC 27001:2013** A.6.1.1 - **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

CYBER FRAMEWORKS



Regulations have a similar development / **lifecycle**

A Program **NOT** A Project

NIST and NERC CIP

NERC CIP

- CIP Requirements
  - CIP-002 – Cyber System Categorization
  - CIP-003 – Security Management Controls
  - CIP-004 – Personnel & Training
  - CIP-005 – Electronic Security Perimeter
  - CIP-006 – Physical Security
  - CIP-007 – System Security Management
  - CIP-008 – Incident Response Planning
  - CIP-009 – Recovery Plans
  - CIP-010 – Configuration Change Management
  - CIP-011 – Information Protection

NERC CIP

Identify	Protect	Detect	Respond	Recover
CIP-002 CIP-003 CIP-007	CIP-004 CIP-005 CIP-006 CIP-010 CIP-011	CIP-005 CIP-006	CIP-008	CIP-009

- CIP Requirements
  - CIP-002 – Cyber System Categorization
  - CIP-003 – Security Management Controls
  - CIP-004 – Personnel & Training
  - CIP-005 – Electronic Security Perimeter
  - CIP-006 – Physical Security
  - CIP-007 – System Security Management
  - CIP-008 – Incident Response Planning
  - CIP-009 – Recovery Plans
  - CIP-010 – Configuration Change Management
  - CIP-011 – Information Protection

CONCLUSIONS

- Utilities have increasing need for better connectivity to a variety of sensors on the edge of the grid.
- These sensors provide excellent situational awareness without having personnel physically located in the substation.
- However, the communication paths between these sensors and utility staff have introduced a new threat to the utility.
- There are a cyber frameworks which can be employed to help identify and reduce cyber threats.
- There are regulations which require certain utilities to implement a cyber security program.
- These practices should be viewed as best practices to reduce the threat exposure and not a guarantee.

Questions?

Presenters

Theo Laughner

E: theo@powergrid-rx.com

P: 865-385-3838

Scott Morris

E: smorris@alchemy-global.net

P: 703-224-3471

T: @ScottMorrisCCIE