A Touch Point on Cyber Security

Common Industry Gaps

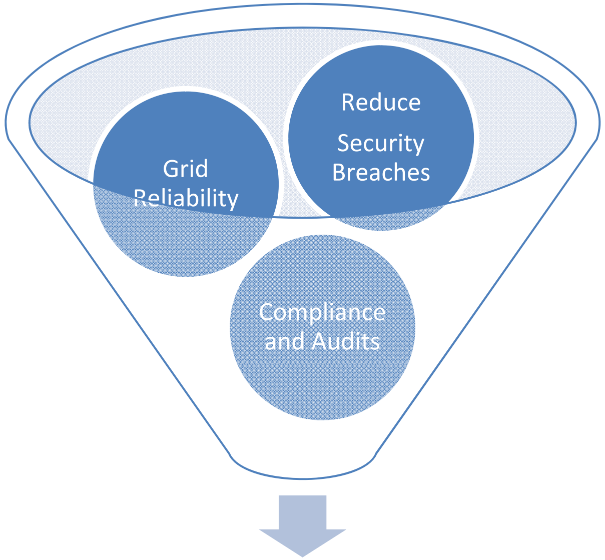
Michael Manske
Senior Security Architect
West Monroe Partners

mmanske@westmonroepartners.com

galvincenter for electricity innovation at ILLINOIS INSTITUTE OF TECHNOLOGY

IEEE PES Power & Energy Society®

How much security is enough?

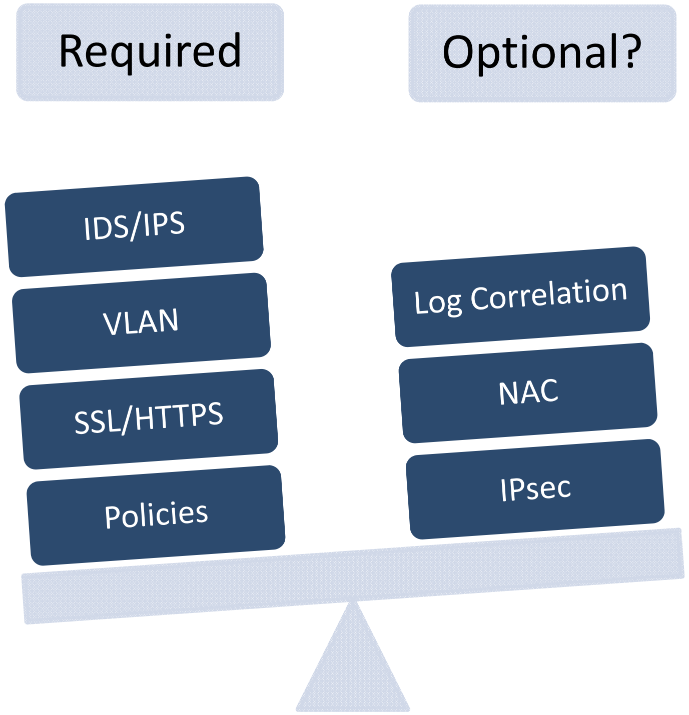


Grid Reliability

Reduce Security Breaches

Compliance and Audits

Cyber Security Main Business Drivers



Required

Optional?

IDS/IPS

VLAN

SSL/HTTPS

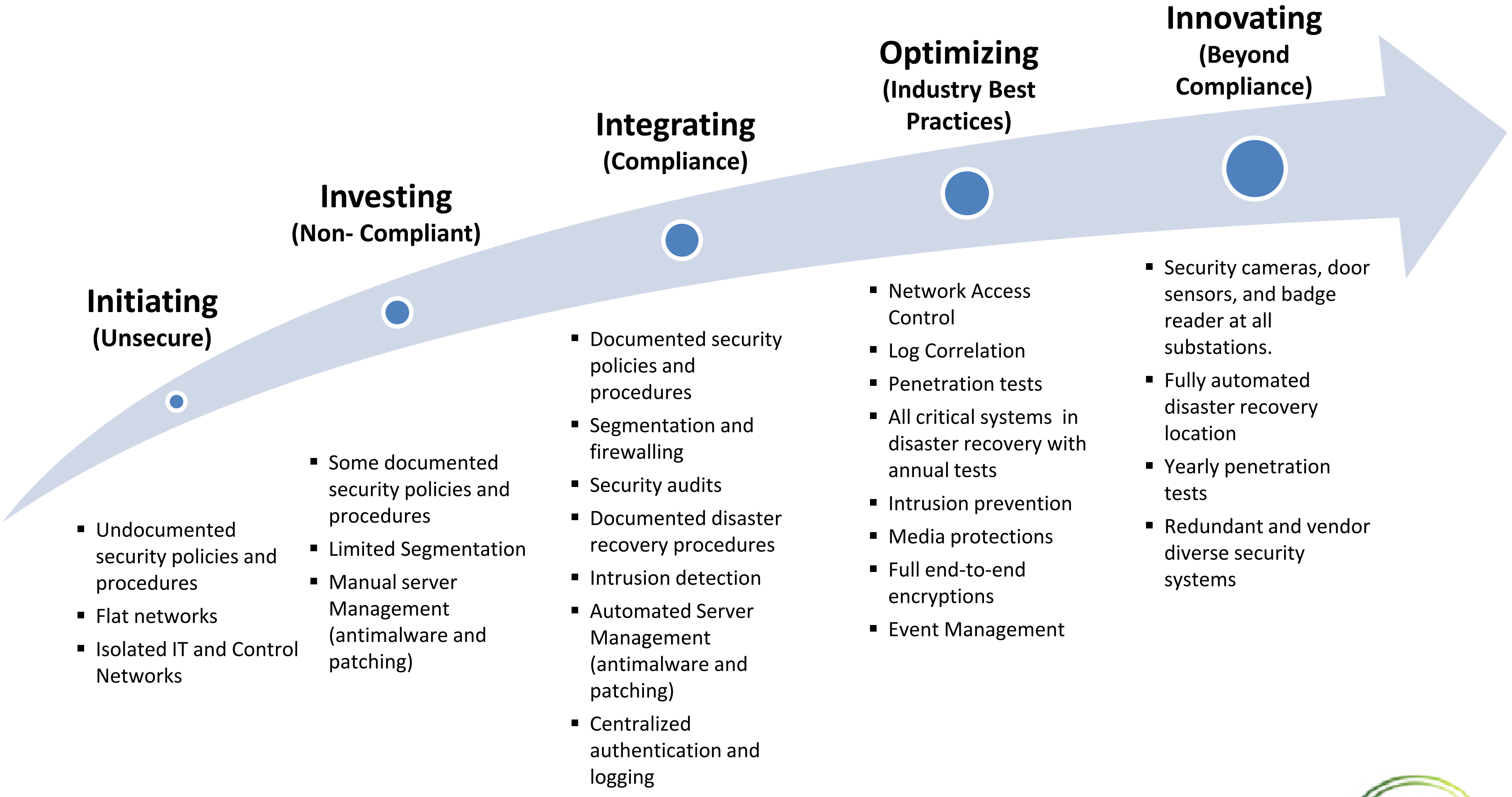
Policies

Log Correlation

NAC

IPsec

Security Maturity Model



Initiating
(Unsecure)

- Undocumented security policies and procedures
- Flat networks
- Isolated IT and Control Networks

Investing
(Non- Compliant)

- Some documented security policies and procedures
- Limited Segmentation
- Manual server Management (antimalware and patching)

Integrating
(Compliance)

- Documented security policies and procedures
- Segmentation and firewalling
- Security audits
- Documented disaster recovery procedures
- Intrusion detection
- Automated Server Management (antimalware and patching)
- Centralized authentication and logging

Optimizing
(Industry Best Practices)

- Network Access Control
- Log Correlation
- Penetration tests
- All critical systems in disaster recovery with annual tests
- Intrusion prevention
- Media protections
- Full end-to-end encryptions
- Event Management

Innovating
(Beyond Compliance)

- Security cameras, door sensors, and badge reader at all substations.
- Fully automated disaster recovery location
- Yearly penetration tests
- Redundant and vendor diverse security systems

Common Industry Gaps (1)

- Cyber Security Vision
  - Failure to have a documented security architecture for the Smart Grid (infrastructure and application integration)
  - Failure to documented all design and cyber security requirements
- Risk Assessment
  - Project implementation proceeding prior to performing risk assessment
  - Failure to mitigate identified vulnerabilities and risks
- Vendor and Device Selection
  - Lack of follow-up to assure vendor adherence to the cyber security standards
  - Failure to document a strong set of cyber security criteria for vendor selection

Common Industry Gaps (2)

- Polices and Procedures
  - Minimum review of policies and cyber security governance
  - Procedures regarding cyber security have not been reviewed and updated
- Security Governance
  - Project teams are not sufficiently familiar with the cyber security polices
  - An organizational chart for cyber security responsibilities has not been created
  - No apparent link between the people responsible for cyber security and management

Common Industry Gaps (3)

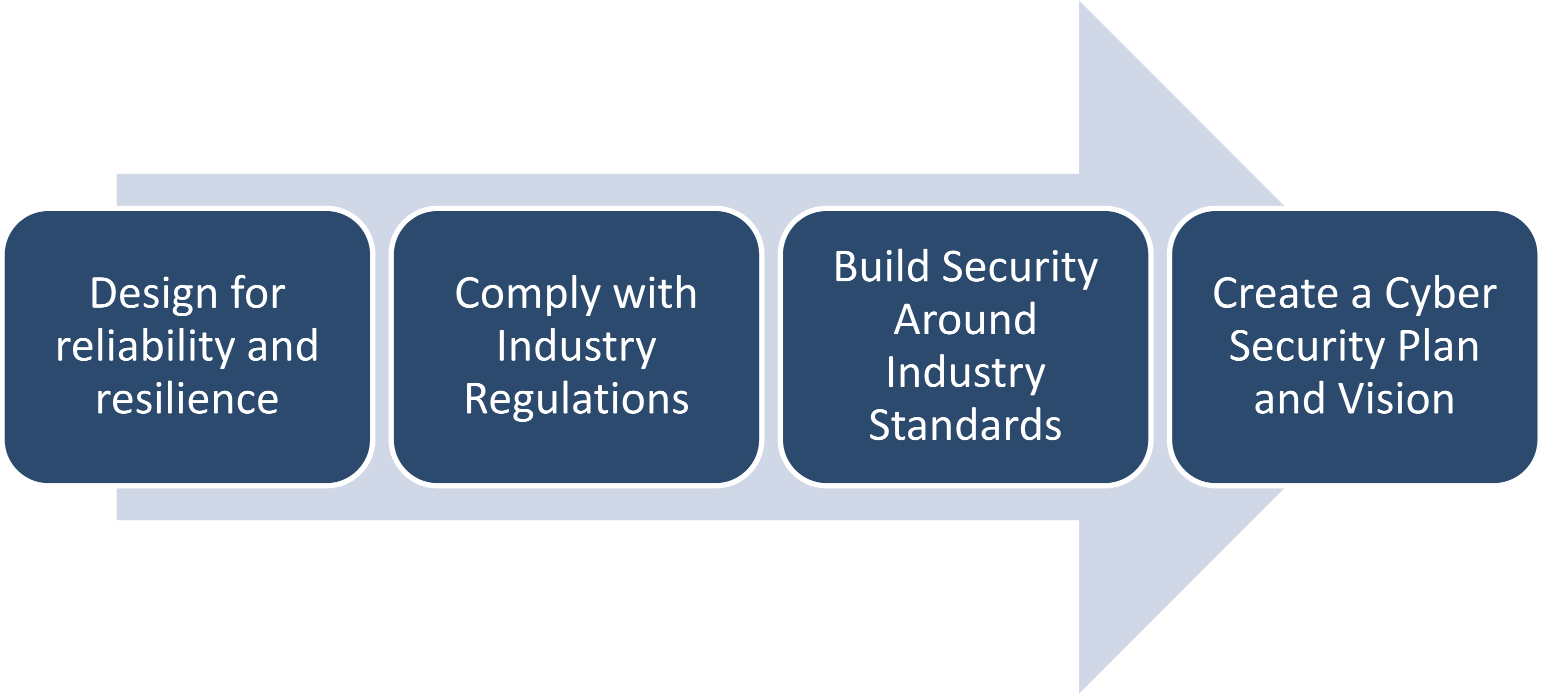
- Network Segmentation and Firewalls
  - No segmentation between corporate intranet and operational network
- Monitoring and Logging
  - Lack of detection and monitoring tools and procedures for monitoring operational networks
  - Failure to log all devices to a centralized location
  - Lack Intrusion Prevention/Detection (IPS/IDS) systems
  - Failure to actively monitor logs and report incidents
- Encryption
  - Identification of appropriate and effective use of encryption and key management technologies

Common Industry Gaps (4)

- Server and Workstation Management
  - Lack of a centralized patch management system
- Passwords and Authentication
  - Lack of centralized authentication
  - Use of default passwords and shared administrative passwords
- Security Assessments and Audits
  - Failure to perform regular vulnerability scans and security assessments (3rd party and internal)
  - Lack of regular and annual reviews of cyber security risks (NIST Methodology) at each phase of the project's implementation
  - Failure to verify vulnerability testing, auditing, and patching testing by the vendors and service providers

Cyber Security Approach

- What should your security approach be?



Design for reliability and resilience

Comply with Industry Regulations

Build Security Around Industry Standards

Create a Cyber Security Plan and Vision