Emerging Cybersecurity Standards for Critical Infrastructure – Lessons from Recent Goals Released by CISA and NIST in the United States

Dr Ilesh Dattani CEng, CISA

Assentian Limited

The Standards Landscape

- Fragmented, Confusing and sometimes even contradictory

- Regulators interpretation of standards
- Guidelines
- Best Practice

Cyber Risk Profile

The Profile is a **unified approach for assessing cybersecurity risk.**

- Consolidates 2,300+ regulations into 277 diagnostic statements
- Gives financial institutions one simple framework to rely on
- Based on common ISO and NIST categories (Identify, Protect, Detect, Respond, Recover)
- Adds two categories specific to the financial industry (Governance, Dependency Mgmt.)

Industry-Wide Harmony

The Profile improves cybersecurity across the entire sector.

The Profile scales to a **firm's impact on the global economy.**

- Only nine questions to determine impact tier
- Fewer, more tailored assessment questions
- Based on systemic impact—not asset size
- Subsequent tier review provides roadmap for advanced security

Institutions

Bringing relief to the entire ecosystem.

- Higher confidence in cybersecurity efficacy
- Common language for the whole industry
- Better understanding across sectors and borders
- Collective action based on common threats
- More innovation, thanks to standardized format to help prove security measures

Assentian Limited

CYBER RISK INSTITUTE

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

- Cross-sector control system cybersecurity performance goals as well as sector-specific performance goals
- Look to provide a single consistent approach taking in controls and guidance from many sources
  - CISA Cyber Essentials
  - CISA Cybersecurity Best Practices for Industrial Control Systems
  - CISA Pipeline Cyber Risk Mitigation Infographic
  - CISA Recommended Practice: Defence in Depth
  - Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards Guidance NRC Draft Regulatory Guidance (DG)-5061, “Cyber Security Programs for Nuclear Power Reactors.” NIST SP 800-82, Rev 2, “Guide to Industrial Control Systems (ICS) Security.”
  - NISTIR 8183, Rev 1, “Cybersecurity Framework Version 1.1 Manufacturing Profile.”
  - ISO 27799, ISO/IEC 27010 - Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications
  - ISO/IEC 27011
  - ISO/IEC 27002
  - ISO/IEC TR 27015
  - ISO/IEC 27001, ISO/IEC
  - 27005, ISO/IEC 27006, ISO/IEC 20000, and ISO 22301

Nine Consolidated Goals

- The nine goals include specific objectives
  - support deployment and operation of secure control systems
    - further organized into baseline and enhanced objectives
- Baseline objectives represent recommended practices for all control system operators
- Enhanced objectives include practices for critical infrastructure supporting
  - national defence;
  - critical lifeline sectors (i.e. energy, communications, transportation, and water);
  - or where failure of control systems could have impacts to safety

Nine Consolidated Goals

- Risk Management and Cyber Security Governance
- Architecture and Design
- Configuration and Change Management
- Physical Security
- Systems, Data Integrity, Availability and Confidentiality
- Continuous Monitoring and Vulnerability Management
- Training and Awareness
- Incident Response and Recovery
- Supply Chain Risk Management

What does it mean ?

- Intended to reflect high-level principles that CI owners should aim to achieve
- Goals are indicative of future cybersecurity standards or regulations
- They are aligned and represent a consolidation of existing standards, guidelines and best practice
- Certain sectors could receive heightened security

Thankyou

Any Questions

Summary Technical Paper on the Goals available end of May 22

Email: ilesh.dattani@assentian.com