The Voice of the Networks

Energy Networks Association

Security Posture Assessment for Operations Technology and Control Systems

Joe Dauncey
Chair, ENA Cyber Security Group, UK
April 2015

About the ENA

- The Energy Networks Association (ENA) represents the ‘wires and pipes’ transmission and distribution network operators for gas and electricity in the UK and Ireland. Our members control and maintain the critical national infrastructure that delivers these vital services into our homes and businesses.
- The ENA's overriding goals are to promote the UK and Ireland energy networks ensuring our networks are the safest, most reliable, most efficient and sustainable in the world. We influence decision-makers on issues that are important to our members. These include:
  - Regulation and the wider representation in UK, Ireland and the rest of Europe.
  - Cost-efficient engineering services and related businesses for the benefit of members.
  - Safety, health and environment across the gas and electricity industries.
  - The development and deployment of smart technology.
- As the voice of the energy networks sector ENA acts as a strategic focus and channel of communication for the industry. We promote the interests and good standing of the industry, and provide a forum of discussion among company members.

About the Cyber Security Group

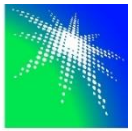
- The aim of the CSG is:
  - To actively assist ENA Member Companies in managing the administrative, engineering and technical aspects of cyber security issues arising from both existing infrastructure and the development and deployment of extensive ICT infrastructure (Smart Grids).
- The CSG will:
  - Report to and take direction from the Strategic Communications Group (SCG);
  - Liaise with DECC, Ofgem, CPNI and other key policy makers and stakeholders as appropriate to inform the work of the Group;
  - Liaise with STEG, SGIS and other key external committees and task groups as appropriate to inform the work of the Group;
  - Liaise with other ENA committees and task groups as appropriate.

The Threat Continuum

TARGET

SandWorm

ارامكو السعودية
Saudi Aramco



Untargeted Commodity Threats e.g. spam, generic malware

Casual External Adversary

Casual Insider

User Error e.g. dataloss event

Skilled Insider

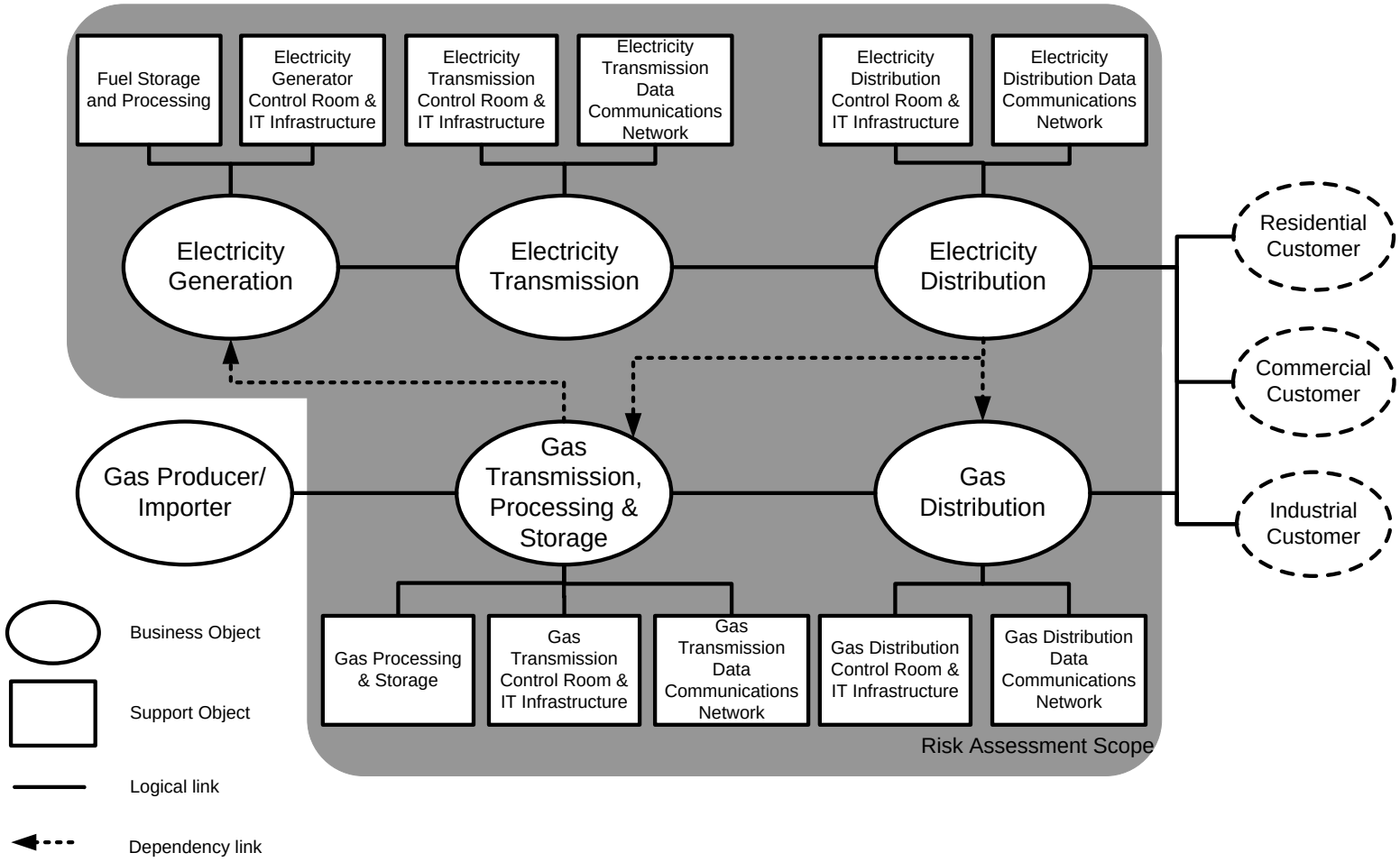
Determined External Adversary

Determined Internal Adversary

Nation State

The problem we are trying to solve …

End-to-End Risk Assessment



Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

- **Challenge**: Develop capabilities to manage dynamic threats and understand cyber security posture of the grid
- **Approach**: Develop a maturity model and self-evaluation survey to develop and measure cyber security capabilities
- **Results**: A scalable, sector-specific model created in partnership with industry

ES-C2M2 Objectives

- Strengthen cyber security capabilities
- Enable consistent evaluation and benchmarking of cyber security capabilities
- Share knowledge and best practices
- Enable prioritized actions and cyber security investments

Ten Domains

RISK Risk Management	ASSET Asset, Change, and Configuration Management	ACCESS Identity and Access Management	THREAT Threat and Vulnerability Management
SITUATION Situational Awareness	SHARING Information Sharing and Communications	RESPONSE Event and Incident Response, Continuity of Operations	DEPENDENCIES Supply Chain and External Dependencies Management
WORKFORCE Workforce Management	CYBER Cybersecurity Program Management		

- **Domains are logical groupings of cybersecurity practices**
- **Each domain has a short name for easy reference**

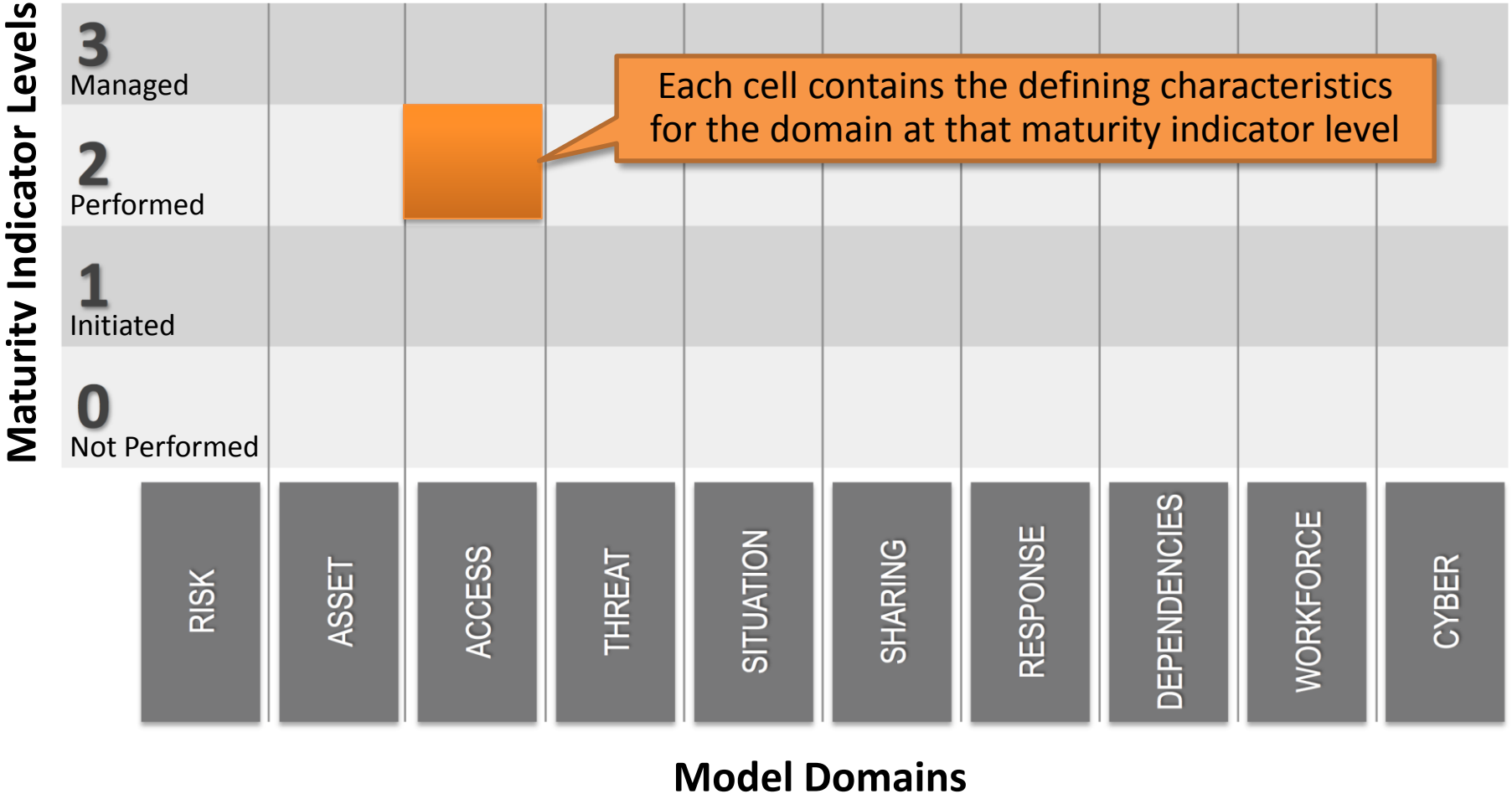
ES-C2M2 Domain Descriptions - Examples

Domain	Description
Risk Management (RISK)	Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders. RISK comprises three objectives: 1. Establish Cybersecurity Risk Management Strategy 2. Manage Cybersecurity Risk 3. Manage RISK Activities
Asset, Change, and Configuration Management (ASSET)	Manage the organization's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives. ASSET comprises four objectives: 1. Manage Asset Inventory 2. Manage Asset Configuration 3. Manage Changes to Assets 4. Manage ASSET Activities

Maturity Indicator Levels

LEVEL • PRACTICES
0 Incomplete • Practice is not performed
1 Performed • Initial practices are performed, but may be ad hoc
2 Planned • Practices are documented • Stakeholders of the practice are identified and involved • Adequate resources are provided to support the process (people, funding, and tools) • Standards and/or guidelines have been identified to guide the implementation of the practices
3 Managed • Practices are guided by policies (or other organizational directives) and governance • Policies include compliance requirements for specified standards and/or guidelines • Activities are periodically reviewed to ensure they conform to policy • Responsibility and authority for performing the practices are assigned to personnel • Personnel performing the practices have adequate skills and knowledge

Model Overview



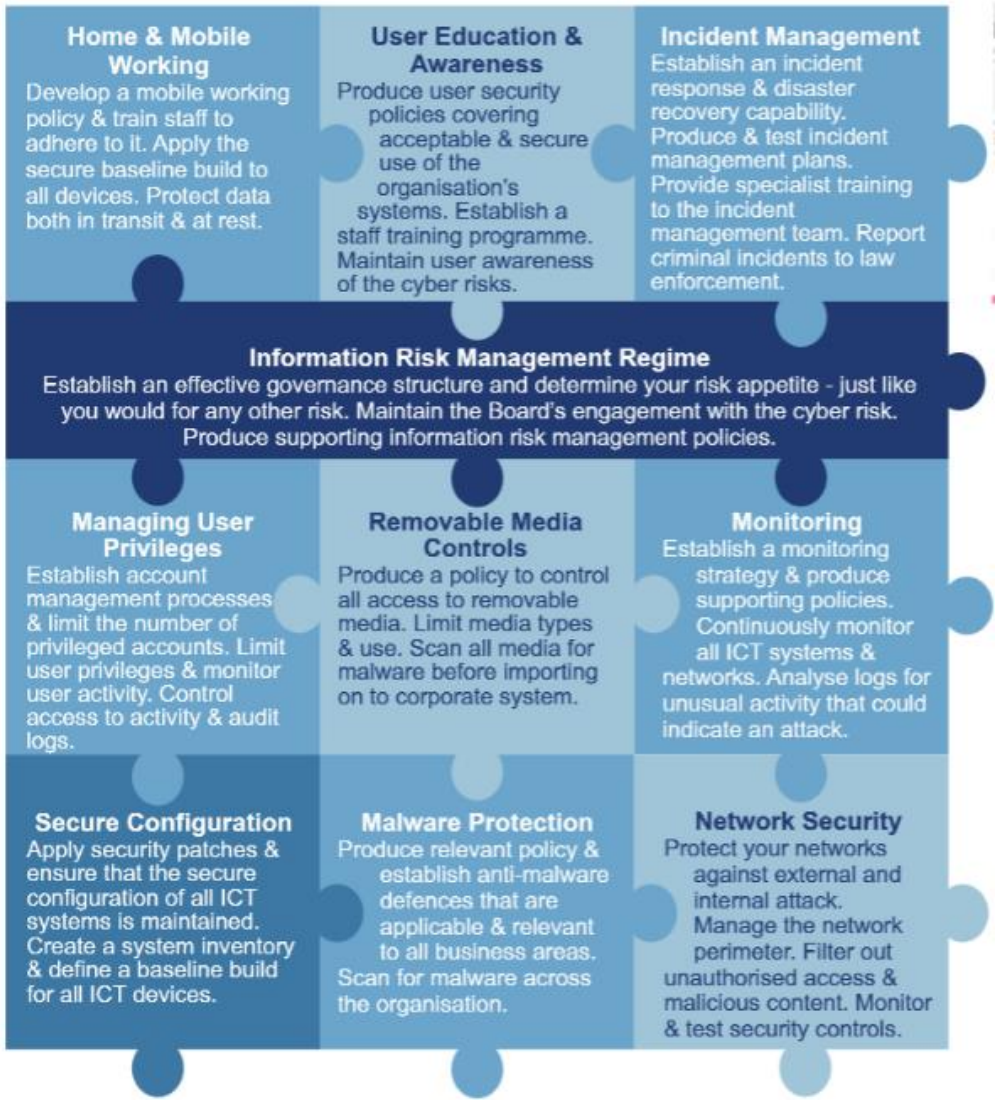
ES-C2M2

Electricity Subsector Cybersecurity Capability Maturity Model

Governance

			Status	Outlook
1	IT Security Programme	• Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus.	G	Neutral
2	Security Communication, Governance & Organisation	• Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus.	A	Improving
3	Monitoring & Protecting our Infrastructure	• Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus.	A	Warning
4	Protecting our Critical Assets	• Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus.	A	Improving
5	Protecting our Sensitive Data	• Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus.	A	Improving

Cyber Essentials



Any Questions?