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



















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**

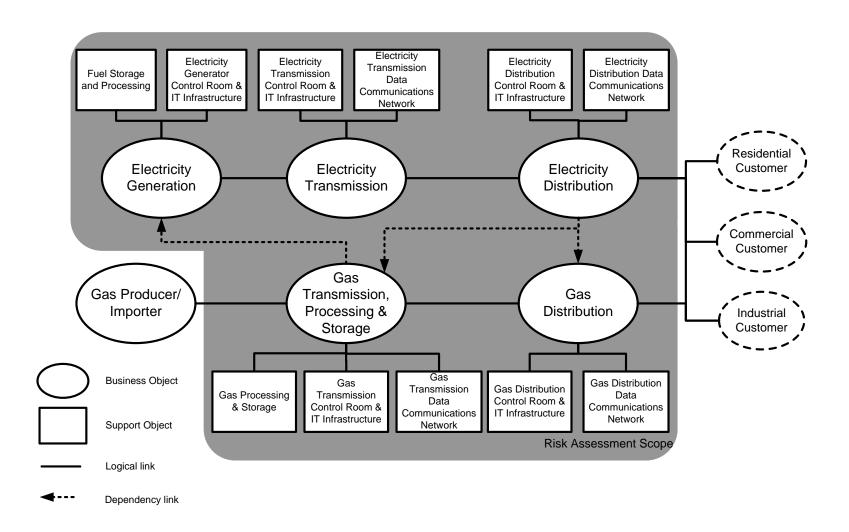
The problem we are trying to solve ...





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, sectorspecific 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

Asset, Change, ACCESS THREAT Threat and Identity and ASSET 쭖 Risk and Access Vulnerability Management Configuration Management Management Management EPENDENCIES Event and Supply Chain RESPONSE SHARING Information Incident Situational and External Sharing and Response, Dependencies Awareness Communications Continuity of Management Operations WORKFORCE Domains are logical groupings of Cybersecurity CYBER cybersecurity practices Workforce Program Management Each domain has a short name for easy Management 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

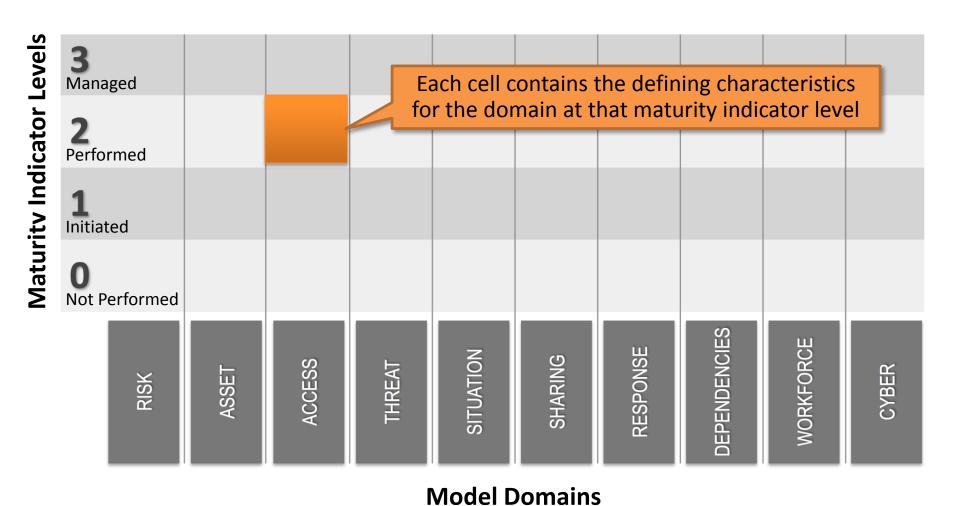
- Practices are documented
- Stakeholders of the practice are identified and involved
- Adequate resources are provided to support the process (people, funding, and tools)
- Standards and/or guidelines have been identified to guide the implementation of the practices

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



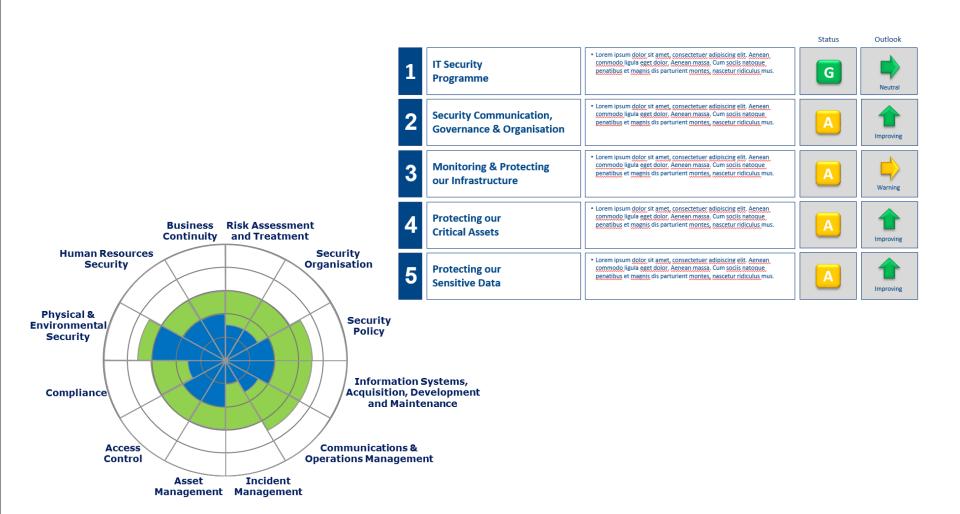
Office of Electricity Delivery and Energy Reliability



Electricity Subsector Cybersecurity Capability Maturity Model

Governance





Cyber Essentials



Home & Mobile Working

Develop a mobile working policy & train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit & at rest.

User Education & Awareness

Produce user security policies covering acceptable & secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Incident Management

Establish an incident response & disaster recovery capability. Produce & test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Information Risk Management Regime

Establish an effective governance structure and determine your risk appetite - just like you would for any other risk. Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

Managing User Privileges

Establish account management processes & limit the number of privileged accounts. Limit user privileges & monitor user activity. Control access to activity & audit logs.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types & use. Scan all media for malware before importing on to corporate system.

Monitoring

Establish a monitoring strategy & produce supporting policies. Continuously monitor all ICT systems & networks. Analyse logs for unusual activity that could indicate an attack.

Secure Configuration

Apply security patches & ensure that the secure configuration of all ICT systems is maintained. Create a system inventory & define a baseline build for all ICT devices.

Malware Protection

Produce relevant policy & establish anti-malware defences that are applicable & relevant to all business areas. Scan for malware across the organisation.

Network Security

Protect your networks
against external and
internal attack.
Manage the network
perimeter. Filter out
unauthorised access &
malicious content. Monitor
& test security controls.

Any Questions?



