CYBERSECURITY

listen to the podcast

THE ENERGY EXCHANGE

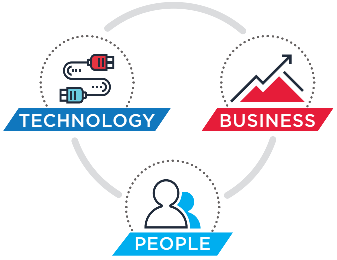
/ Concise and actionable intelligence for today's most relevant Grid Modernization topics

Significance—*Why does this matter?*

Our grid, one of the most complex machines in the world, is a critical infrastructure. Industrial control systems (ICS), such as SCADA Systems that manage the grid, can be targets for cyber-attacks, which can create not only inconveniences but impact commerce, well-being, and safety. Protecting grid systems from vulnerabilities and mitigating the risks should be at the forefront of every utility today. The traditional methods of protecting IT assets are not by themselves adequate protection for critical OT assets.

Structure—*What do I need to know?*

The following is based on the DOE Cybersecurity Capability Maturity Model (C2M2) Program. The Energy Sector C2M2 (ES-C2M2) was developed to address the unique characteristics of the electricity subsector.



TECHNOLOGY CONSIDERATIONS

- *Compliance to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards is not enough.*
- *Public C2M2 model can be used for facilitated or self-assessment of cybersecurity capabilities.*
- *OT/IT technology convergence requires understanding the very different cyber challenges faced by IT versus OT systems.*
- *Effective cyber processes and solutions:*
  - *Determine the risk profile and vectors.*
  - *Establish a rigorous process around managing assets, communications and services.*
  - *Establish a cybersecurity framework that addresses all aspects of the environment.*

> "The Three Laws of SCADA Security:
>
> - Nothing is secure;
> - All software can be hacked;
> - Every piece of information can be an attack."
>
> ANDREW GINTER
> *VP of Industrial Security, Waterfall Security Solutions*

BUSINESS CONSIDERATIONS

- *Cyber is a critical business function, it warrants the highest level of attention in the organization.*
- *Develop an ongoing process to identify and manage continuing risk.*
- *Cyber-protection must be a factor at the onset of a program and inherent in the design, it cannot be effectively added afterward.*
- *Many cyber risks must be managed and mitigated, including damages that are financial, physical, personnel and reputational.*

PEOPLE CONSIDERATIONS

Utility-Centric (Internally Facing)

- *Following proper cyber practices is not an option it is a requirement, e.g. controlled use of admin privileges, secure configuration of hardware, software, workstations and mobile devices, and continuous audit processes.*
- *OT systems evolving in the Internet of Things (IoT) environment face cyber threats that previously isolated systems did not.*
- *Cyber-awareness and diligence are everyone's obligation, attacks can come through seemingly innocent actions, e.g. opening email attachments, inserting USB sticks, allowing coat-tailing into secure areas, etc.*

Customer-Centric (Externally Facing)

- *Customer facing websites must protect customers' financial, energy usage, and Personably Identifiable Information (PII) data.*
- *Connections to customer-owned electric vehicle chargers, solar PV, energy storage, and smart inverters exposes security vulnerabilities and introduces cyber risks for customers, utilities, and third parties.*
- *Resilient, cybersecure access to electric power is a mission critical need for virtually every industrial, business, and residential customer.*

Steps—*What do I do now?*

To measure progression, maturity models typically have "levels" along a scale — the DOE's ES-C2M2 model uses a scale of maturity indicator levels (MILs) 0–3 for each domain, which are described below. A set of attributes defines each level. If an organization demonstrates the specified attributes, it has achieved both that level and the capabilities that the level represents within a specific domain. Having measurable transition states between the levels enables an organization to use the scale to: define its current state; determine its future, more mature state; and identify the capabilities it must attain to reach that future state.

MATURITY INDICATOR LEVEL (MIL)	DESCRIPTOR	DESCRIPTION
0	LACKING	*No practices in place*
1	BASIC	*Practices performed, but ad hoc*
2	INSTITUTIONALIZED	*Practices documented; Stakeholders identified; Resources allocated to support process*
3	MANAGED	*Activities guided by policies and governance; Compliance requirements specified; Policies reviewed regularly to ensure conformance; Responsibilities and authorities are assigned; Personnel assigned have knowledge and skills*