ARMEXA

Case Study:

Advancing IT/OT Security Maturity Across a Multi-BU Energy Organization

Armexa partnered with a leading energy company operating across regulated and non-regulated sectors, including utilities and oil & gas. The client sought to elevate its IT/OT cybersecurity maturity through a structured, scalable governance program. Armexa was engaged to lead four strategic workstreams aimed at building a comprehensive OT security framework, assurance mechanisms, and technology deployment strategy.

Industry:
Utilities, Oil & Gas

Location:
North America

Services:

- **Governance, Risk, and Compliance**
- **Technology Roadmap**
- **Technology Engineering & Design**
- **Technology Deployment**

Challenge: Design a cybersecurity program that could scale across diverse environments

The client operates across a complex landscape of business units, each with distinct operational models, regulatory obligations, and levels of cybersecurity maturity. This includes both regulated entities such as utilities, and non-regulated facilities with varying degrees of OT security implementation.

The primary challenge was to design a cybersecurity governance program that could scale across this diverse environment while remaining practical, achievable, and aligned with industry standards. The solution needed to account for differences in risk profiles, organizational structures, and technology readiness, while ensuring consistency in policy enforcement and control implementation.

Additionally, the client required a framework that could integrate seamlessly into existing workflows across M&A activities, operations, and capital projects. This meant addressing not only technical gaps but also organizational readiness, role clarity, and long-term sustainability of the program.

Solution: Armexa Developed a Buy/Build/Run OT Cybersecurity Governance Program in collaboration with the Client's Team

The program included documentation such as policies, standards, and job aids, lifecycle objectives and program implementation procedures. The program was structured around four key workstreams:

- **Workstream 1: Risk Assessment Methodology, Controls Framework, Standards Management**
  - Defined an OT Security Framework aligned with NIST, IEC 62443, and CIP standards
  - Selected applicable controls for non-CIP facilities based on risk reduction and industry best practices
  - Designed a tailored OT Security Policy and supporting standards

- **Workstream 2: Assurance Framework for M&A, Operations, and Capital Projects**
  - Established organizational roles and responsibilities to ensure long-term adherence to the framework
  - Defined expertise and training requirements for site and BU focal points

- **Workstream 3: M&A Deep Dive and Gap Assessment**
  - Conducted a post-deal OT cyber risk review and proposed an ongoing framework
  - Performed a Gap Assessment at a selected facility to evaluate alignment with the OT Security Framework

- **Workstream 4: Technology Selection and Pilot/POC Deployment**
  - Collaborated with the client to select and deploy a risk-mitigating technology at a pilot facility
  - Delivered high-level and low-level designs, staged and implemented the solution, and provided ground-level support

Impact:

The program resulted in the successful rollout of the OT Cybersecurity Governance framework across all business units, with a pilot implementation in the client's gas BU. Key outcomes included:

- A scalable and achievable OT security framework tailored to both regulated and non-regulated environments
- Development of reusable templates for NIST-aligned policies and standards
- Enhanced organizational readiness through clearly defined roles and training pathways
- Initiation of technology deployments that support compliance and risk mitigation

ARMEXA