ARMEXA

Case Study:
Advancing OT Cyber Risk Assessment Through CyberBowtie Methodology Development

A large U.S. based energy operator sought to modernize its approach to OT cyber risk assessment by adopting a structured, repeatable methodology capable of quantifying cyber physical risk across complex operational environments. The organization engaged Armexa to design and deliver a customized CyberBowtie assessment framework, integrated into the Sphera PHA Pro platform, to enhance security measure evaluation, strengthen risk communication, and align cybersecurity practices with enterprise risk tolerance criteria.

Challenges

The client required a cyber risk assessment method that could bridge the gap between traditional process safety practices and emerging OT/ICS cybersecurity challenges. Existing assessment processes lacked consistency, did not fully account for cyber initiated threat scenarios, and offered limited ability to quantify likelihood in a transparent, defensible way.

Key obstacles included:

- Inconsistent documentation of threats, safeguards, and consequences across sites.
- Difficulty aligning cyber scenarios with corporate risk matrices designed for physical process hazards.
- Limited integration between cybersecurity analysis and existing PHA work processes.
- Need for a scalable approach that could support multiple facilities and diverse industrial systems.

Industry: Energy & Industrial Operations

Environment Operational technology environments with cyber physical systems, process units, and safety critical industrial control systems leveraged across multiple facilities.

Armexa Services:

- OT Cyber Risk Assessment
- Bowtie Analysis & Methodology Development
- OT/ICS Cybersecurity Program Design
- FAIR-Based Likelihood Modeling
- PHA-Pro Integration & Template Development
- Cybersecurity Workshops & SME Facilitation

Our Solution

Armexa developed and delivered a tailored CyberBowtie methodology, toolkit, and operational workflow purpose built for OT cyber physical risk assessment. The solution included:

- **Custom PHA Pro CyberBowtie Template & Library**
  A governed template and safeguard library designed to standardize threat modeling, consequence analysis, and safeguard evaluation across OT environments.
- **Quantitative Likelihood Model Using FAIR Based Principles**
  Integration of structured likelihood factors—threat frequency, source, exploitability, and difficulty—with annualized event rate calculations aligned to the client's corporate risk matrix.
- **Three Day Facilitated Workshop**
  Armexa SMEs conducted onsite working sessions to guide assessors through scenario development, template use, safeguard effectiveness evaluation, and Bowtie diagram completion.
- **Automated Linkage to Corporate Risk Tolerance Framework**
  Built in logic to translate likelihood and consequence severity into consistent residual risk ratings using the client's approved Cybersecurity Risk Tolerance Matrix.
- **Knowledge Transfer & Documentation**
  Delivery of a comprehensive operations manual, reference materials, and hands on training to equip internal cyber assessors for ongoing, scalable use of the methodology.

Outcomes & Impact

The engagement resulted in a fully operational OT cyber risk assessment methodology adopted across the client's organization. Key benefits included:

- **Repeatable, Defensible Assessments**
  A standardized approach that ensures consistent interpretation of cyber threats, safeguards, and risk outcomes across teams and sites.
- **Improved Alignment Between Cybersecurity and Process Safety**
  Integration of cyber initiated events into established PHA processes strengthened communication between OT, IT, and risk stakeholders.
- **Enhanced Risk Visibility**
  Built in reporting and visualization tools enabled clearer understanding of residual risk and prioritization of mitigation efforts.
- **Scalability Across the Enterprise**
  The customized template, governed safeguard library, and structured methodology support roll out across additional operational units and future assessments.
- **Accelerated Assessor Capability**
  Through training and documentation, internal teams gained the ability to independently manage assessments and maintain the methodology.

ARMEXA

Ready to talk all things cybersecurity?
Contact us at info@armexa.com

armexa.com