Schneider Electric

Business Brief

Schneider Electric's Critical Infrastructure and Security Practice (CISP) is a global leader in cyber security services, providing comprehensive security solutions.

Benefits

Our clients have requirements larger in scope than secure products alone can provide. We have a comprehensive solution portfolio that includes:

- Products designed with security
- Compliance with industry standards
- Cyber security experts and delivery/ support personnel
- Enhanced solutions to meet client cyber security program needs

Our cyber security solutions will meet the challenging industrial landscape. We are the largest and most experienced ICS cyber security practice in the industry.

Advantages

- Platform Independent: CISP's security solution portfolio will work on ANY control system platform.
- Network Agnostic: CISP's security solution portfolio can be deployed on any network topology or technology, independent of network lifecycle, due to the lifecycle methodology of the solution portfolio.
- Industry Relevant: CISP's portfolio is applicable to any industrial manufacturing industry, whether the focus is on cyber security compliance or network systems optimization.
- Solution Ecosystem: CISP is greater than the sum of its parts: cyber security consulting, network compliance, regulatory experts, auditors, network systems design, and implementation.

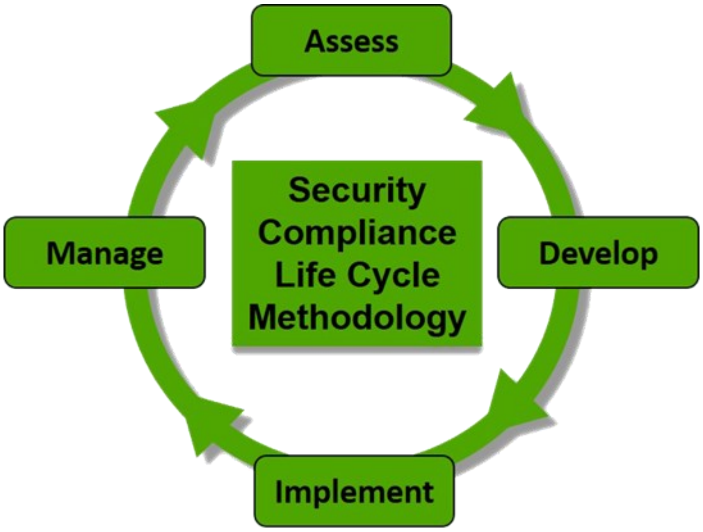
Oil/Gas

The global oil and gas industry is a large, expansive segment that consists of upstream (drilling and exploration), midstream (transportation between the pipelines and the refineries), and downstream (refining, processing, and distribution). As diverse as these segments may seem within the oil and gas industry, they all share two specific elements—every country in the world lists oil and gas as critical infrastructure and they all share a common cyber threat. In 2012, 41 percent of energy companies were targets for cyber criminals, so it is no wonder that several of the world's major oil and gas producers have fallen victim to devastating cyber attacks, as that number has continued to increase each year.[1] The Shamoon virus demonstrated that the world's largest oil and gas companies are not immune and that cyber threats can come from inside a plant[2] as easily as from the outside. Such events have only helped to further fuel the need for more government support for compliance as well as increased industry requirements and corporate mandates to prevent cyber attacks. Even intellectual theft is a risk, as some hackers have been able to access oil and gas companies' handbooks and geologic data.[1] And political hacktivist groups have targeted oil and gas companies as a form of protest for using the dollar in oil trades.[3]

Whether it is upstream, midstream, or downstream, all three divisions have the need to secure facilities against cyber security events that can disrupt production and threaten facilities and risks to safety. Because the oil and gas industry has three sub-segments that each function differently with unique needs and regulations, there is a need for a comprehensive yet adoptable cyber security program. As with any project undertaking such as cyber security, the first step is to identify the risks to help define the needs that will ultimately identify the compliance requirements, providing the operators the key actionable items in the plan to move to the next step to identify their unique technical requirements and specifications. Simple point solutions are ultimately a "one size fits all" approach, when in fact every facility and plant owned by a single company is unique, requiring a plantwide comprehensive cyber security solution that is flexible enough to address any individual facility's needs.

Many companies may already be at some point in the development of a cyber security program or are just embarking on the process. To facilitate these needs, the Schneider Electric cyber security consulting team has developed their portfolio of cyber security solutions using their Security Compliance Life Cycle Methodology. This approach permits the cyber security consulting team to engage with a client at any point in their own program's lifecycle. If the project is brand new, the cyber security consulting team would start with the Assessment stage. If it is mature and already in place, the cyber security consulting team can begin at the Management stage or any point between.

The security compliance lifecycle approach consists of these four tenets:



Assessment
The cyber security consulting team reviews the current network, identifies any problems or issues, and suggests areas for improvement.

Development
Using an assessment or plan as a guideline, the cyber security consulting team identifies what needs to be implemented and develops the detailed designs required to make it happen.

Implementation and Modernization
The cyber security consulting team takes the network design and turns it into reality through the procurement, staging, and commissioning of the client's new system or system upgrades.

Management and Optimization
The cyber security consulting team manages the network closely, providing a mechanism to improve and optimize the continuously changing landscape of network usage.

The Schneider Electric cyber security consulting team is a global consulting organization that provides comprehensive cyber security compliance and solutions regardless of industry. The cyber security team's solutions are system- and plant-agnostic and are adaptable to any industry and region.

[1] www.cfr.org
[2] http://www.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idUSBRE8860CR20120907
[3] http://gulfnews.com/business/technology/anonymous-plans-global-cyber-attacks-on-energy-firms-on-friday-1.1348396

To learn more about Invensys' Critical Infrastructure and Security Practice (CISP) solutions,
contact your sales representative or visit: http://iom.invensys.com/CyberSecurity

Schneider Electric
Schneider Electric • 1820 Preston Park Blvd, Suite 1900, Plano, TX 75093 • Tel: 1 (613) 591-1943 •
Fax: 1 (613) 591-1022 • www.schneider-electric.com

Rev. 201401