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.

Power

The global power generation industry is a large industry comprised of power generation from fossil fuels, nuclear, and an array of renewable energy sources. Every global region has identified power generation as part of their critical infrastructure and has recognized the need to secure it. It is no secret that power plants are under ever-increasing cyber threats. ICS-CERT reported that of 256 cyber incidents reported for the year, 151 were identified by the energy sector—59 percent.[1] For this reason, most countries have adopted either government regulations or regional compliance standards that provide guidance to power generation companies. Regardless of fuel types, all power generation facilities have both a need and a mandate to secure their plants from cyber threats that could cause power outages and result in regional disruption. The power generation industry is not a newcomer to cyber security regulations, and in many regions there already exists cyber security standards that are being adopted by other countries.

However, many of these regulations are not prescriptive, leaving the individual operators with the daunting task of developing and implementing a cyber security program on their own. In most cases this results in a reliance on singular hardware and software point solutions such as firewalls and anti-virus software—leaving them with a false sense of security. After all, who is going to install, configure, maintain, and patch these items? 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

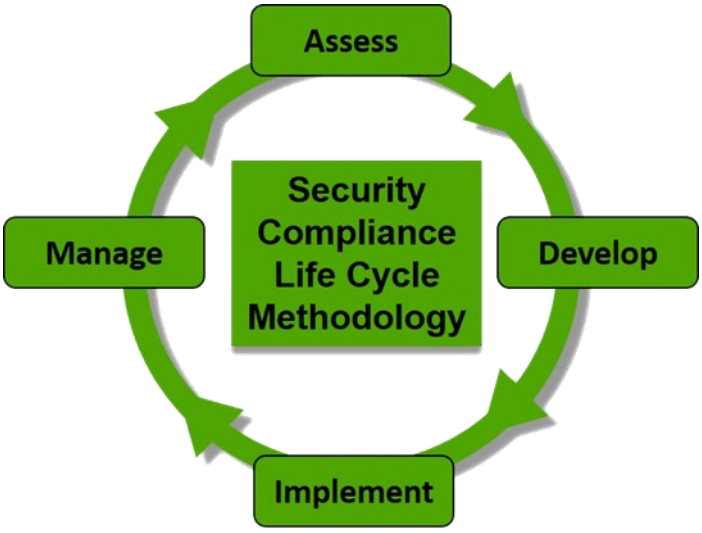
Management stage or any point between. The security compliance lifecycle approach consists of these four tenets:

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] https://ics-cert.us-cert.gov/monitors/ICS-MM201312

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