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.

Water and Wastewater

Clean water has long been identified globally as a critical natural resource. It should be no surprise that every country on the globe has also identified the water and wastewater industry as part of their country's critical infrastructure. The U.S. Department of Homeland Security has recognized the water and wastewater sector as "essential to the nation's public health and safety, economic vitality, and way of life."[1] At the same time, the Repository for Industrial Security Incidents (RISI) reports that "cyber attacks [are] up by 60 percent at water utilities."[2] With the evolving cyber security threat landscape, and as top global critical infrastructure, cyber security is a top priority among these facilities. Virtually every country has identified cyber security threats against the water and wastewater industry and realizes the need to protect their processing facilities and distribution infrastructure from potential cyber security threats. Until they do, they risk the possibility of not just a facility shutdown but also disruptions in operations and risks to public safety through the water supply. Cyber events could cause a reduced flow in water from fire hydrants or even the release of untreated sewage into the public water supply.[1]

Water and wastewater facilities require cyber security and with a revolving regulatory landscape, the first step towards securing these facilities is a comprehensive cyber security compliance program that identifies risks and needs. Many of today's wastewater and water regulations are not prescriptive, leaving the individual operators with a nearly impossible 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.

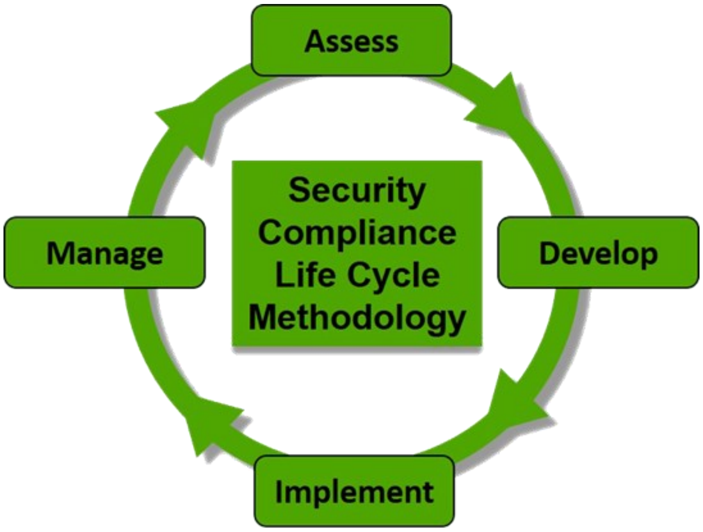
Many companies may already be at some point in the development of a cyber security program or are just embarking on the process. To facilitate these needs, the Schneider Electric cyber security consulting team has developed their portfolio of cyber security solutions using their Security

Compliance Lifecycle Methodology. This approach permits us 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.phoenixcontact.com
[2] http://www.wateronline.com/doc/cyber-attacks-up-by-percent-at-water-utilities-0001

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