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.

Smart Cities

Smart cities are one of the newest global innovations that will touch nearly every aspect of the consumer's life, bringing the service(s) provider, industry infrastructure, and consumer all together. More than 130 smart city projects are underway worldwide that are focused on innovations in transportation and urban mobility.[1] The smart cities market, which includes transportation, energy, water, and waste management, focuses on energy efficiency, increased sustainability, and reduced gas emissions and use of natural resources.[2] The smart city ecosystem is a broad partnership between both the public and private sector. City planners, developers, and non-governmental organizations, IT system integrators, software vendors, energy and utility providers, the automotive industry, and facility control providers, as well as technology providers for mobile technology, cloud computing, networking, Machine-to-Machine (M2M) and Radio-Frequency Identification (RFID), all have a role to play.[3] Along with all of these partnerships is the need to develop comprehensive cyber security standards that address very broad and complex interoperability of the smart city ecosystem. Smart city developers are looking to cyber security resilience to be the baseline.[3] The World Economic Forum defines cyber resilience as "the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery."

Smart city cyber security must address a broad risk analysis due to the highly connected nature of the systems and the risk factor that brings. Systems can suddenly fail from one critical point of weakness.[4] Many services like hospitals, transportation, and home security are at risk of being compromised as they become more digital and interconnected.

Smart cities will require a holistic and robust cyber security program. A comprehensive cyber security compliance program that identifies and categorizes risks and maps them to specific needs is key. Such cyber security framework exists today—the NIST Framework is one such compliance program. 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. The key reason being, 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 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.

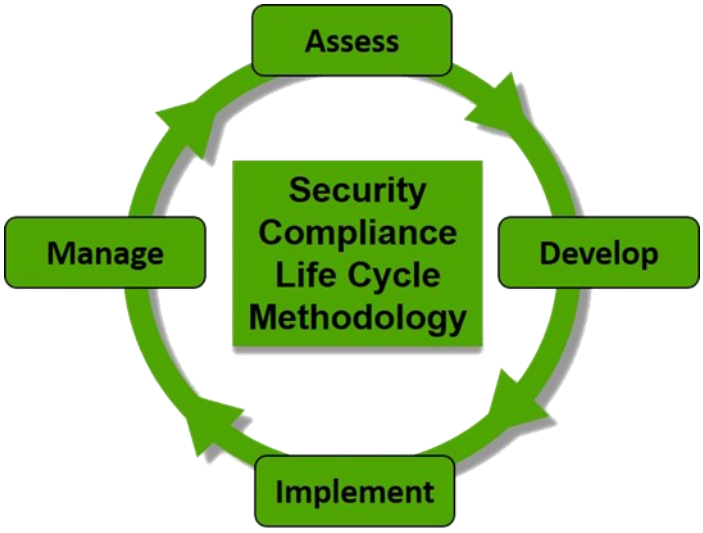
The security compliance lifecycle approach consists of these four tenets:

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] http://green.tmcnet.com/topics/green/articles/2013/03/04/329041-smart-city-projects-worldwide-focus-urban-mobility.htm
[2] http://www.forbes.com/sites/sarwantsingh/2014/06/19/smart-cities-a-1-5-trillion-market-opportunity/
[3] Transformational 'smart cities':cyber security and resilience, Symantec
[4] http://www.newrisk.com/smartcities.html

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