Cyber Security Services
Compliance Solution Sheet

Summary

Schneider Electric’s Cyber Security Services team has identified seven key cornerstones of cyber security:

1. Identification of Critical Assets
2. Electronic Access Controls
3. User Access Controls
4. Patching
5. Anti-Virus and Device Control
6. Disaster Recovery
7. Logging

Once the items above have been identified, we implement our lifecycle methodology using four distinct phases:

1. Assess
2. Develop
3. Implement
4. Manage

Business Value

Our Cyber Security Cornerstones Assessment includes an on-site and hands-on review of the customer’s facility. We work closely with Control Staff, Operation Technology, IT, and Security Team to review and study:

- Current risk posture
- Applicable standards or regulatory needs
- Network security perimeter
- Patch management process
- Backup and recovery procedures
- Anti-virus status
- Operational critical assets

7 Cornerstones of Cyber Security

Every customer has something they need to protect, regardless of region or industry. We work directly with customers, leveraging our cyber security lifecycle methodology. We have identified seven critical cyber security cornerstones that provide a foundation every customer will benefit from, whether they are starting a cyber security program from scratch or reassessing an existing one.

1. **Identification of Critical Assets**
   Critical assets are the items that are essential to business continuity. If these items are destroyed, damaged, or tampered with, it would negatively impact the safety and reliability of the network, facility, or equipment. This often leads to loss of revenue and consumer confidence.

2. **Electronic Access Controls**
   Electronic access controls can include equipment like firewalls to help detect and block intruders trying to gain unauthorized access to critical company assets. Other forms of electronic access control can include application whitelisting or physical security measures such as key card access.

3. **User Access Controls**
   User access controls can help prevent network interruption by ensuring users are only able to access certain areas of the network. Using a “least privilege” methodology prevents users from accessing confidential company data as well as inadvertently or maliciously tampering with network settings.

4. **Patching**
   A patch is a piece of software designed to fix security vulnerabilities and other bugs and improve the usability or performance of systems and software. Patching closes security holes in applications that computer hackers and viruses can exploit.

5. **Anti-Virus and Device Control**
   Anti-virus software and device control policies help prevent malware and malicious cyber events from taking the network offline. Device control policies can extend to USB drive usage and other removable devices to minimize insider risks such as data loss and malware introduction.

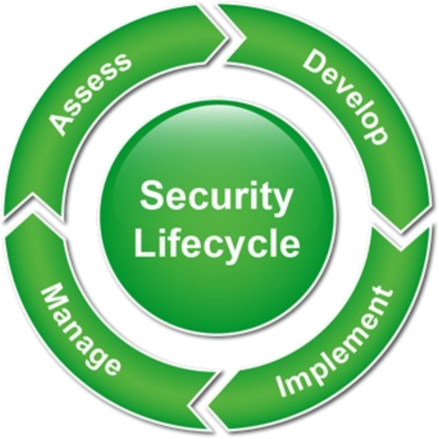
6. **Disaster Recovery**
   Backups refer to the various strategies and procedures involved in protecting a database against data loss and reconstructing the database after any kind of data loss. A backup is a copy of data from a database that can be used to reconstruct that data. Backups can be divided into physical backups and logical backups.

7. **Logging**
   Logging is integral in ensuring an ICS is secure and stays secure. It can show when, where, and how a security intrusion was attempted and if it was successful. Logging is also a company’s necessary audit trail that is required for some industry and government regulations.

Almost any cyber security requirement (whether corporate mandate or government/industry regulation) stems from these seven building blocks. Using these building blocks, the Cyber Security Services team can determine what the customer needs in order to set them up for success with their cyber security program. Once the requirements have been identified, we implement our lifecycle methodology, outlined below.

Cyber Security Services Lifecycle

We use our unique lifecycle approach, which consists of four key stages: Assess, Develop, Implement, and Manage, allowing us to engage any customer at any point in their own cyber security program. The solutions that we deliver are platform-agnostic and focus on helping customers with their cyber security compliance requirements. All of our solutions are hardware, software, and product independent.



Stage 1: Assess
The Cyber Security Services team works with the customer to assess their current network to help identify problems and develop requirements.

Stage 2: Develop
The Cyber Security Services team uses the assessment and the customer's requirements to develop a program unique to their needs.

Stage 3: Implement
The Cyber Security Services team implements the network design from procurement through staging and commissioning of the cyber security solution.

Stage 4: Manage
The Cyber Security Services team manages the network closely, providing a mechanism to improve and optimize the continuously changing landscape of network usage.

Our team can help equip organizations with up-to-date, comprehensive cyber security solutions to meet any requirement or regulation, whether it is company-mandated, industry-specific, government-issued, or merely a matter of best practices. Our experience in process automation environments allows our team of experts to deliver platform-agnostic solutions that help the client bridge the IT gap. All of our solutions are hardware, software, and product independent.

To learn more about Schneider Electric Cyber Security Services, contact your sales representative or visit:
http://software.invensys.com/services/security-and-compliance-services/cyber-security-services/

Schneider Electric • 1650 W. Crosby Rd Carrollton, TX 75006 • Tel: 1 (972)-323-1111 • www.schneider-electric.com

Rev. 201507