Cyber Security Services
Compliance Solution Sheet

Cyber Security Lifecycle Methodology

Summary
The Cyber Security Services team can engage any customer at any point in their cyber security program, whether they are just starting out or need to enhance their current security posture. Our core solutions are based on our lifecycle methodology, which consists of four phases:

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

Business Value
Using the seven cornerstones of cyber security as a foundation, we use our lifecycle methodology to create 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.

Our unique lifecycle methodology allows us to engage any customer at any point in their cyber security program, regardless of their industry or regulatory landscape. Using this methodology, we can adapt to the customer's needs to develop customized solutions to get them where they want to be. The lifecycle methodology consists of four key stages: Assess, Develop, Implement, and Manage. These four steps are not only critical to developing a holistic cyber security solution, but they also outline critical points of our client engagement.

Stage 1: Assess

The starting point for any engagement is the assessment. This is where the Cyber Security Services team works closely with the client to assess their current network to help identify problems and develop requirements. The goal of the assessment stage is to define a risk-based assessment of the client's network in order to develop what the true needs of the client are. As an example, if a client wants three firewalls installed, the first questions are:

Stage 1: Assess (cont.)

- Why are firewalls determined to be the best approach?
- How was the quantity of three determined?
- Who determined the locations of the firewalls?

In many cases, this is putting the proverbial cart in front of the horse. A risk-based assessment determines what the client needs to protect and the level of risk is appropriate for the network asset in question. Keeping control room connectivity is probably a higher priority than keeping power to the break room. This type of assessment helps the client to determine what their actual needs are versus their wants.

The assessment is also an important element of most regulatory programs and plays a crucial role in most companies in determining budgeting.

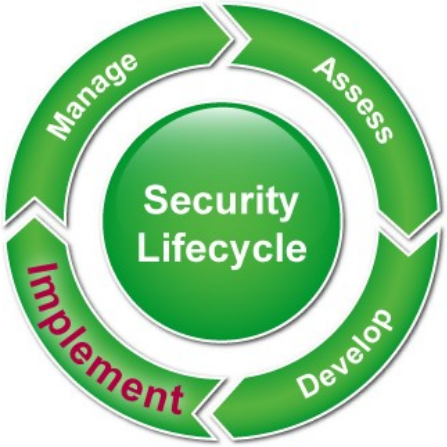
Stage 2: Develop

After the Assessment phase is completed, the next stage is the development phase. As the name implies, the Cyber Security Services team uses the assessment and the customer's requirements to develop a program unique to their needs. Prior to jumping right into network designs, it is important to develop a program that addresses not just the technology but also the timing. Our typical client does not always have the necessary downtime to implement all the changes that are required. In these cases, we can work with clients on a technology roadmap to the defined solution priority based on time windows. We understand the nature of our clients' industries and that "rebooting" the network is not always an option.

With project timing addressed, we can move onto network design. Here, we defer to our clients' preferences for hardware (switches, firewalls, etc.) and software (anti-virus, malware prevention, etc.). In situations where the client does not have a preferred vendor, we recommend one of the "best-in-class" vendors we typically work with. The conclusion of the Development stage is a truly comprehensive cyber security solution that addresses not just the client's unique needs but also their timeline as well as internal corporate mandates, such as preferred vendors.

Stage 3: Implement

With the Assessment and Development stages complete, the next stage is implementation. At this point, Cyber Security consultants implement the network design from procurement through staging and commissioning of the cyber security solution. This is a very unique point for the Cyber Security Services team. Unlike many Cyber Security consultants that will come in and do a report or assist on a network design, our Cyber Security Services team will actually perform the cyber security solution implementation and cut over. The Cyber Security Services team has not only cyber security knowledge but the industry and control expertise to be able to work seamlessly onsite, interfacing with both the process team as well as the IT team as needed.



Upon completion of the installation, the Cyber Security Services team provides a full set of documentation for the site-specific solution that was just delivered.

Stage 4: Manage

In many cases, the Implementation stage would be seen as the final step. However, in cyber security, the most important phase is always the management stage. At this stage, we manage the network closely, providing a mechanism to improve and optimize the continuously changing landscape of network usage. Many companies skip or just ignore the management step altogether, believing that their cyber security elements will now protect them going forward. This might be true if the company never makes any changes after the cyber security solution went in; however, this is not practical, as today's process control networks are dynamic. There are always changes, patches, adds, and drops going on.

These daily operational exercises run the risk of compromising the security of the network. Management provides the means to be able to monitor changes, track updates, and detect unconditional behavior alerting you to a potential issue before it can become an event. Stage 4: Management is by far the most important stage to help ensure network integrity.

Our lifecycle methodology is flexible enough that it can be used in its entirety or implemented by any individual solution set, providing a comprehensive yet scalable solution for cyber security compliance.

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