ARC VIEW

NOVEMBER 5, 2015

Implementing Advanced Cybersecurity Measures at a Major Global Energy Company

By Shin Kai

Keywords

Cybersecurity, SecurePlant, IT/OT, ITIL, SLA

Overview

Even today, with all the front page headlines about serious cybersecurity breaches, many managers in industrial plants and other critical facilities face significant headwinds when it comes to obtaining approval to fund effective ongoing cybersecurity projects. ARC Advisory Group hears stories about an increasing feeling of helplessness among professionals responsible for implementing and maintaining industrial cybersecurity measures and programs.

Nobody denies the importance of cybersecurity measures nowadays, but many industrial companies still find it challenging to budget the resources needed to develop, deploy, and maintain appropriate measures.

Yokogawa Electric executives recently briefed ARC Advisory Group about how Cisco Systems and Yokogawa worked with Shell to co-develop the company's "SecurePlant" cybersecurity solution for its control systems. While Shell is one of the largest and most technologically advanced global energy majors, ARC believes that case studies such as these can be informative for even small-to-midsize companies. This is partly because cybersecurity case studies are so scarce, and also because the achievements of large, sophisticated global companies such as Shell may provide models for others to follow. .

Key takeaways from the briefing include:

- Industrial organizations should regard cybersecurity measures in the context of ongoing risk management, rather than isolated countermeasures, to help ensure business and operations continuity.
- Companies should team with external information technology (IT) and operational technology (OT) partners that have the appropriate respective domain expertise.

- Establishing a solid information management plan is important to promote a phased investment and technology deployment based on the company's business requirements and scale.
- Appropriate investments in cybersecurity can help change risk into an opportunity cost.

The SecurePlant Solution

At the 2015 ARC Industry Forum in Orlando, Florida in February, Yokogawa announced a collaboration with Cisco to deliver Shell's SecurePlant initiative, a comprehensive security management solution for plant control systems jointly developed by Cisco, Yokogawa, and Shell. According to the announcement:

- Yokogawa and Cisco collaborated with Shell on the design of the SecurePlant service. The objective of these services is to standardize patch management, anti-virus protection, and other security practices at Shell plants around the world – many with a variety of control systems and equipment from different vendors (and often multiple generations of the same vendors' systems). The two companies will jointly deploy the solution and provide operational services for Shell.

- Supplier-certified Windows security patches and virus signature files will be distributed from a centralized SecureCenter to the local SecureSite at each plant via Shell's existing global network. Proactive, real-time monitoring capabilities will enable centralized management of plant security. A customer help desk, operated jointly by Yokogawa and Cisco, will be available 24/7/365 to manage solution-related incidents.

Development Process

As ARC learned, Shell's senior management drove this initiative, spurred by the company's need to further secure the Windows-based computers embedded into its Yokogawa DCSs and other industrial automation systems. (According to Yokogawa executives, Shell was a leader in embracing this type of transformational technology within its automation systems.) Significantly, Shell's approach to cybersecurity looks at the problem from a risk management perspective to help ensure business continuity, social responsibility, and environmental responsibility.

Shell's initial project with Yokogawa focused on a single site to establish and fine-tune the appropriate measures. This enabled Yokogawa to accumulate extensive expertise in appropriate countermeasures to address a wide range of security vulnerabilities in industrial automation. These include (but are not limited to) firewalls, access control, network monitoring, and disaster recovery system backup.

Shell's approach to cybersecurity looks at the problem from a risk management perspective to help ensure business continuity, social responsibility, and environmental responsibility.

Unlike centrally managed enterprise IT systems that utilize corporate standards, most industrial control systems are managed independently at each site. Having different management approaches represents a challenge for achieving a consistent level of security. This explains the need for an approach that addresses vulnerabilities by mitigating exposure for the business as a whole of potential and appropriate risks. Shell's upstream and downstream operations encompass multiple sites around the globe, with some in very remote locations.

In 2011, Shell began working with the OT specialists at Yokogawa and the IT specialists at Cisco to develop a standard, centralized approach for industrial patch management, anti-virus protection, and other security practices to enhance the cyber security of the company's diverse base of control systems. To accommodate the often remote locations of these Shell sites, the security management service would have to managed and supported remotely from a central location.

Yokogawa and Cisco collaborated to develop the prerequisite secure, remote connectivity solution that is appropriate for mission-critical real-time control systems.

Shell appropriately named this industrial cyber security management initiative "SecurePlant." While challenging for both Yokogawa and Cisco, ongoing strong support from Shell executives and the companies own IT specialists, helped drive this important initiative forward to realization.

By including cybersecurity measures as an integral element in a company's comprehensive approach to risk management for business continuity – rather than an isolated project – the company believes that it can transform risk into business opportunity.

Yokogawa recognizes that many industrial organizations have limited internal IT and OT resources. But if those organizations identify and partner with best-in-class IT and OT companies, they can take advantage of that respective expertise to work together to build business platforms that embed appropriate cybersecurity measures, procedures, and strategies processes into the organization's existing systems and business processes.

How IT and OT Companies Collaborate

ARC asked Yokogawa how, as a leading OT supplier, it worked together with leading IT-supplier, Cisco, to share resources and information when collaborating to execute the Shell project.

According to Yokogawa, there are two stages in Shell's centralized remote monitoring project: the system implementation stage and the post-implementation support stage.

Implementation Stage

During the system implementation stage, Cisco has primary responsibility for supplying and configuring the infrastructure for remote monitoring, while Yokogawa has responsibility for integrating appropriate hardware into Shell's operational control systems to enable secure connectivity with the infrastructure.

Operational Stage

Once the connectivity between central system and local operations has been established, the project enters the operational support stage. This includes monitoring the delivery of OS patches and anti-virus pattern files for control systems and establishing and managing a help desk operation that is available 24 hours a day, 7 days a week, 365 days a year. Yokogawa supports both OT hardware and application software in the remotely monitored plants via the help desk, with Cisco specialist on call if any trouble should occur in any of the Cisco-implemented infrastructure-related areas.

In addition to building a robust fundamental hardware-software system by multiple redundant architectures to achieve minimal system downtime, collaboration was established among team members to ensure business continuity as much as possible through the ITIL and SLA operations.

Ensuring Business Continuity

Through close collaboration among team members – including Shell corporate and local plant personnel, Cisco personnel, and Yokogawa personnel -- the project participants succeeded in building a robust fundamental hardware-software system architecture. This architecture employs multiple redundant configurations to minimize system downtime. On that foundation, the solutions offered are supported by an Information Technology Infrastructure Library (ITIL) to help align IT best practices with the needs of the business in the case of a problem with the exchange of information or if a cyber attack has been detected, and a service-level agreement (SLA) to help ensure appropriate performance and uptime for business continuity.

SMBs Can Also Benefit

With its well-proven VPSRemote solution, extended in 2012 to work with IT-type systems as well with as the company's CENTUM DCS and ProSafe-RS safety systems, Yokogawa has considerable experience supporting its global customer base with remote diagnostics, maintenance, application, engineering and other secure remote services. From a technical perspective, this is a similar to the approach that Yokogawa and Cisco employ for the Shell SecurePlant solution, which uses some of the same technology.

According to the company, Yokogawa's global customer base for Industrial Automation (IA) systems includes approximately 26,000 systems, spanning a wide variety of geographical locations, industry sectors, applications, degrees of criticality, and cybersecurity requirements. These customers include a large number of small-to-medium businesses (SMBs) in addition to large multinational enterprises like Shell.

For further information or to provide feedback on this article, please contact your account manager or the author at skai@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.