Control, Instrumentation and Automation in the Process and Manufacturing Industries

IML

April 2015

CONTROL ENGINEERING EUROPE

www.controlengeurope.com

A smart and intuitive way to increase productivity

The Festo route to Industry 4.0

Profinet diagnostics: organisational issues

Determining measurement uncertainty

Taking a collaborative approach to cyber security

Taking a collaborative approach to cyber security

At the last Yokogawa user conference, Tyler Williams, manager PCD IT security for Shell Global Solutions, who is responsible for cyber security activities in automation and control system environments, explained the company's cyber security journey. *Suzanne Gill* reports.

Cyber security is an important consideration for all companies today, yet it is also an issue that can pose many problems, especially for a company the size of Shell.

One of the challenges to overcome when creating an enterprise-wide cyber security strategy and framework is cost. Williams explained one way this challenge was addressed at Shell: "There is, generally, a focus on risk reduction as the indicator of value, or benefit, when evaluating the wide range of cyber security investment options. For an organisation with the size, scale and complexity of Shell, these investment costs were non-trivial and difficult to quantify consistently to the wide range of business stakeholders around the world - especially when these expenditures could mean the sacrifice of other plant, or organisational investment priorities. Our approach, therefore, was first to do the math, and align cyber security investment with business objectives and communicate our cyber security strategy to management as an enabler for future growth and value creation, not simply as a cost center, or line item expense."

Shell has a goal of becoming the most innovative technology company in the world. Leveraging IT is an important area to help it achieve this across its automation and control systems. "We have reduced the amplification of the cyber threat language of our cyber security messaging and have instead made a point of treating cyber security as an enabler for new business opportunities, such as remote or managed engineering services," said Williams. Adopting such a philosophy provided a convincing argument that the implementation of cyber security standards could have a positive effect in helping the company to meet its goal.

Understandably, Shell comprises many complex business models with different operating units in different lines of business treating risk differently. "They will naturally all have differing business drivers, investment priorities and vendor communities," explained Williams. "For example, in some business lines within Shell, the responsibility for managing cyber security in operational environments lies within the IT domain while in others it is handled by engineering. This variability presented us with multiple challenges when setting out to achieve an overarching and standardised cyber security strategy, not to mention when setting out to standardise technical solutions."

Simplify the variables

Williams went on to explain that before any technical solutions could be found it was first necessary to simplify and address all of these variables. "We needed to blend the engineering and IT worlds from the outset of the project. Organisational and technical change issues, regional and global cultural and competency differences, generational disparities, and different ways of working needed to be addressed and overcome. It was vital that we got these factors connected and aligned before moving forward."

How did Shell achieve this seemingly impossible task? Williams highlighted some of the key points.

"It was first necessary to harmonise the language of risk. Different areas of the industry perceive risk differently, and so will perceive any chosen standard differently." The fact that automated systems are becoming more interconnected with the office domain does pose a risk and barriers need to be put in place. "At Shell we had to make the nomenclature of cyber risk management, more engineering specific to ensure it was properly understood and embraced," said Williams.

He went on to emphasise the importance of getting the basics right first. Shell needed to take the many variants of cyber security standards and practices used across the company and reduce them to just one – and then

embed this single set of basic security requirements into their supply chain of automation and control system suppliers (Buy Secure), their portfolio of capital investment projects (Deploy Secure) and current operating assets (Run Secure)... "Any security controls or security features/functionality you impose on your supply chain, then needs to be embedded and monitored into the design and deployment phases of your projects, and then again, maintained as you hand-over to operations. To be successful in this effort, you must start first with a single voice of authority, asking for a single, and simple set of requirements, to suppliers, contractors and staff alike. If you ask too much, you'll break from the start. If you want to implement 100 controls, best to start with 10 and focus on getting them embedded and operating effectively across the lifecycle, then, and only then, should you start adding.

Bridging the divide

"The most important aspect of setting up a cyber security solution is to ensure that all your engineers respect the fact that IT can bring a different, capable set of skills to the table," continued Williams.

Shell has tackled the traditional IT/engineering divide through training. In partnership with other energy and petrochemical companies, it has created a basic set of competencies that will be required of the next generation of engineers and IT staff, which will form part of a new external certification programme called the Global Industrial Cyber Security Professional (GICSP). The areas covered include general IT; IT security; and process automation and control. It is hoped that this move will result in a supply of people who will not only be able to help improve IT security in automation and control system environments but will also be able to design the next generation architectures more quickly with greater robustness built in. They will understand cyber security risk management from an IT perspective and will also understand basic engineering design and operating principles for industrial and automation system environments. "These are the perfect credentials for helping us to continue our security journey," said Williams.

With the organisational foundations established, the next step for Shell was to embed the same principles into their partner community and develop an ecosystem of cyber security technology partners which include companies from the OT and IT domains. This resulted in Yokogawa, traditionally a provider of automation and control system products to Shell, cooperating with Cisco to co-develop and commercialise a new cyber security technology platform called SecureOps – a solutions platform and managed service to support the centralised management and automation of cyber security practices such as access control, asset inventory management and patching and AV services, and sold to Shell under the name SecurePlant.

Williams said: "We are a multi-vendor environment and with this solution in place, we can now work together > p32

with all our suppliers leveraging a single access management platform to securely connect to, and maintain security controls on our industrial automation and control systems. This will certainly help us better manage and maintain security in our industrial environments. With standardised and secure third-party remote access, we can also enable the accelerated adoption of new value added remote engineering services, from our supply chain."

Greg Carter, director of the IoE services group at Cisco, explains more about the joint solution offered by Cisco and Yokogawa. "A successful cyber security solution relies on bringing together the IT and Operational Technology (OT) worlds. Over the past year Cisco and Yokogawa have worked together to develop secure operations in line with Shell's requirements.

"In doing this we realised that Shell's cyber security issues were by no means unique and this resulted in the two companies partnering in the creation of a product and service solution that can be jointly taken to market."

The solution will revolve around a security control framework designed specifically for industrial environments. It consists of a security architecture to support the security control framework, together with the knowledge of how to put them in place in a standardised way and then to manage them.

It will provide a clear and simple regularly updated view of the assets in the environment right down to the patching and anti-virus management – which can be presented as dashboard reports to facilitate compliance and risk management.

"We needed to include anti virus and patch management capabilities because so many of the servers that run control systems are out of date in terms of operating systems," said Carter. "Having a regular, automated way of gathering patches and getting them to remote sites is critical. We will not simply push patches to the control system, but will deliver them to a known point of contact at each site in a repeatable way and will produce dashboards and reports to show that the patches have been delivered. This allows operators to control their own risk."

The service also offers the possibility of having 24/7 remote monitoring of security events as well as the state of the infrastructure and applications that support the entire solution.

Yokogawa and Cisco collaboration in more detail...

The official announcement relating to the collaboration between Yokogawa Electric Corporation and Cisco Systems to deliver Shell's SecurePlant initiative was announced at the recent ISA World Industry Forum.

SecurePlant - a comprehensive security management solution for plant control systems - was jointly developed as an initiative between the three companies involved. There is an agreement to proceed over the next three years with the implementation of SecurePlant at around 50 Shell plants globally.

Industrial producers around the world face a wide range of operational challenges in areas such as cybersecurity that pose a pervasive threat to safety and availability. However, many companies with global operations still take a relatively simplistic plant-by-plant approach, such as implementing operating system security patches and anti-virus pattern file updates. As a result, there is often a large degree of variation relating to plant security levels across an organisation.

In the general practice of control system security management, individual control system vendors extensively validate security patches and anti-virus pattern files to confirm that they do not interfere with system operation, and then report the results to their customers for implementation. Because plants tend to use a variety of control systems and equipment from different vendors, occasionally with multi-generation platforms from a single vendor, this process is often complicated. For this reason, plants increasingly have the need for plant-wide integrated services that take a more holistic and efficient approach to the management of system security.

The SecurePlant solution is designed as a standard solution that consists of the delivery of OS patches and anti-virus pattern files for control systems and the provision of real time and proactive monitoring of solution delivery, as well as a help desk operation to manage this solution.

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

Yokogawa and Cisco now intend to continue to offer comprehensive security solutions involving the deployment, operation, and monitoring of control system environments. These joint services are applicable to plants of all sizes in a wide variety of industries, including facilities spread out over a large geographic area. In addition, both companies will utilise their technologies and experience to develop deep industrial automation (IA) solutions such as remote system maintenance, remote plant asset management and Big Data on the top of a secure remote access platform to help companies make faster decisions, reduce total cost of ownership (TCO), and achieve operational excellence.