Secure Industrial Networks with Cisco

According to the Department of Homeland Security, 53 percent of cybersecurity incidents in the 6 months ending May 2013 were in the energy sector. And the number of attacks is increasing. Are you ready?

Forward-looking oil and gas firms believe today’s turbulent market landscape provides an opportunity to gain competitive advantage by harnessing new technologies. They see opportunity to achieve operational efficiencies and growth through digital technologies powered by the Internet of Everything. Digital strategy and business strategy are becoming one and the same.

Security as a Catalyst for Transformation

Digital transformation means that new and diverse devices are connecting to oil and gas industrial networks. These connections generate greater amounts of data. When managed effectively, that data delivers the right information to the right place at the right time. And this fuels competitive advantage.

With the Internet of Everything, the exploding number of devices and applications are also creating more attack vectors for bad actors to exploit.

Oil and gas companies need to replace traditional approaches like physical segmentation and security by obscurity. They need an integrated approach where information flows in real time to enable immediate action.

Cybersecurity doesn’t need to be an inhibitor. It can be the catalyst for new ways of working. It can help oil and gas companies work more safely and better protect the environment. It can make processes more efficient. Increase production. Reduce costs.

Address the Entire Threat Continuum

Cyberattacks occur on a continuum of before, during, and after. Cisco addresses this entire continuum with our visibility-driven, threat-focused, and platform-based security model.

- Visibility-driven means we are delivering a real-time accurate picture of the network, devices, data, and applications with which we can control the environment and mitigate threats.
- Threat-focused means we identify threats based on understanding normal and abnormal behavior. With contextual awareness, we identify false-positives and assess the impact of a threat. We make decisions and respond rapidly.
- Platform-based means we have an integrated system of agile and open platforms that cover the network, devices, and the cloud. It is a true platform of scalable, easy-to-deploy services and applications. You gain powerful end-to-end visibility with centralized management for unified policy and consistent controls.

Cisco has one of the broadest set of solutions covering the attack vectors and taking advantage of both global and local intelligence.
Securely Converge IT and OT

As oil and gas companies embrace the Internet of Everything, they bring together the use of information technology (IT) and operational technology (OT). OT and IT systems each has its unique security management requirements. IT and OT need to align their strategies and work closely together to ensure end-to-end security. Physical security solutions reduce unauthorized system access and complement the cybersecurity systems in order to protect networks, devices, applications, users, and data.

With the Cisco® Risk Control Framework for Process Control Networks, we can help oil and gas companies implement recognized standards such as the ISA/IEC-62443 for secure industrial automation and control systems.

Cisco Is Doing It Today

The Cisco Secure Ops Solution helps oil and gas companies to secure their industrial control networks. Cisco Secure Ops combines technology, processes, and managed services. It is built on a strong risk-control framework for process-control networks. With Cisco Secure Ops it easier to:

- Manage cybersecurity risk
- Implement and maintain security controls
- Manage secure access to the process-control network
- Support security compliance

Shell has deployed the Cisco Secure Ops Solution to increase security maturity level by improving its cybersecurity and risk management, while lowering costs of delivery and operations (Figure 1).

**Figure 1.** Cisco Risk-Control Framework for Process-Control Networks
Next Steps

The unique Cisco lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.

Cisco and its partners can help to maximize your experience and return on investment from the planning to building and managing of your Cisco Secure Ops solution Secure Industrial Network. Cisco Services provides expert consulting and integration services to help ensure your successful implementation.

For More Information

Find out about Cisco Connected Oil and Gas solutions by visiting http://www.cisco.com/go/oilandgas or contact your local Cisco Sales Representative.