From the ICS frontlines: Approaching OT cybersecurity

EDDIE HABIBI, PAS Global; and **JACOB LAAS GLASS,** Total

To secure industrial facilities and ensure safe and reliable production, operational technology (OT) and information technology (IT) security—traditionally two separate disciplines with different priorities—must collaborate to share cybersecurity and risk management best practices. We recently reached out to a panel of industry experts focused on OT cybersecurity risk mitigation and asked them to share their strategies for making industrial control systems more secure. The firsthand experience collected comes from experts across a diverse range of industries, including oil and gas, chemicals and refining, and power generation. Their essays illustrate the importance of understanding similarities and differences between IT and OT environments.

In this article, we share an excerpt of the Ebook, *Advice for CISOs: How to Approach OT Cybersecurity.* Despite the title, the information presented is useful for anyone involved in protecting OT environments.

As the industrial control system (ICS) industry gives more consideration to cybersecurity, vendors must develop a more holistic view. For now, many companies must contend with an OT environment that is complex and difficult to secure. Several practices have greatly improved cybersecurity environments.

Begin with a technical standard of critical security elements. OT control systems often require multiple components to work together to perform a control function. Every device in that control system can have a critical safety impact on the overall system's function. When a device is installed, all the ways it can negatively impact the system must be evaluated. The same strategy should be applied to evaluating an ICS from a security perspective.

Begin with a technical security standard that the system and its components must meet. One industry security expert said, "Every time we install something, we apply a Swiss cheese model against the standard. We look at it to see what can be set up initially, what we can prevent, what we can detect, what we can respond to and what we can recover. If there is something we cannot do, we look for what we can alternatively do in the system to cover for that security element." When something is added to the system, one way or another, the system must still meet the standard of critical security elements.

When in doubt, assume a protection is not there. Systems are usually well-documented from a cabling standpoint. However, documentation of device configuration is often poor. New technology that detects OT devices and their configurations has been a tremendous help in providing greater visibility, but areas of uncertainty remain. For example, it may be unclear if a device is configured with a host firewall. In this scenario, it should be assumed that it is not there, and then a plan for hardening that device or network must be developed. This involves a lot of work and help from vendors. Some vendors know how to protect their own systems, but others do not get involved in industrial security. A company may have to fulfill this requirement on its own.

Establish an OT department that works closely with the IT department. This gives OT personnel access to IT personnel, who typically have more detailed technical knowledge about cybersecurity issues. In one organization, the OT department resides in the IT department but is still responsible for operations and OT security. The proximity to IT personnel has numerous benefits. Every time a device is connected, different information from the vendor states what is possible and what is not. This helps create good, secure solutions.

Having a security standard for control systems and working with IT to help implement them has proven very effective. "Someone can just sit in their security officer chair and say, 'No, that is impossible,'" the industry security expert said. "We have to make it possible. That is the whole point with OT. We have to make it possible because a significant amount of money is involved."

Stop by the PAS booth (#19) in the exhibition hall to meet the team and learn more about PAS Cyber Integrity™. ●

EDDIE HABIBI is the Founder and CEO of PAS Global. He is a pioneer and a thought leader in the fields of industrial control systems (ICS) cybersecurity, the Industrial Internet of Things (IIoT), data analytics and operations management. In 2017, PAS was recognized in CRN's 15 coolest industrial IoT companies, and Mr. Habibi was listed by CRN as one of the 30 Internet of Things Executives Whose Names You Should Know. He is the co-author of two popular best practices books on operational risk and safety management: *The Alarm Management Handbook* and *The High Performance HMI Handbook.* Mr. Habibi holds an engineering degree from the University of Houston and an MBA degree from the University of St. Thomas.

JACOB LAAS GLASS is the Head of Industrial IT and Infrastructure for Total TEPDK. His first position at Maersk Oil, recently acquired by Total, was as an Instrument/Automation Engineer in 2006. Since then, he has been involved in numerous projects, including the installation of ICS on oil-producing platforms. He has also worked in the telecom and manufacturing execution systems (MES) side of ICS, moving to OT security. He played a key role in establishing guidelines and corporate standards for the company. In 2017, he was asked to lead a team of OT specialists dealing with OT security, critical infrastructure, real-time data, analytics and predictive maintenance. In 2018, he became Head of Industrial IT and Infrastructure, completing the discussion around IT/OT convergence. Today, both the OT and IT specialists are within the same team.

HURRICANE, continued from page 3

site reliability and stability; and detection of technical and software gaps in current software for data analytics.

The technical gaps discovered include effective benchmarking for prioritizing bad actors, advanced filtering of potential bad-acting assets, data analytics for mechanical and equipment issues, automated diagnostics and root cause identification, and automated recommendations for improving loop performance.

Software gaps include more effective time series and before/after visualization, on-demand comparative analysis of process control assets, context visualization and filtering for instrumentation and equipment and valve monitoring, and enterprise-wide benchmarking for prioritization. ●