IT/OT Convergence Means Greater Resources for Both

Robert Landavazo 7/11/18 IIoT

Many of us are familiar with the infamous video of the hacking at the Ukrainian power station in December, 2015 that caused a blackout impacting a quarter million people in the area. As the hackers remotely took control of their workstations, the plant systems operators could do little more than record for posterity the activity that they saw on their PC screens with their mobile phones. So now, any of us can go over to YouTube and watch in horror along with the operators as their cursor moves around their screen, maliciously clicking commands and tripping breakers in various substations. Of significant interest, as they helplessly watch the screen activity that was advancing their power station inevitably toward doom, we hear one operator say to the other "We should call the IT guys," to which his colleague quickly replies "What if it's the IT guys doing this?"

I'd like to give kudos to both gentlemen—the first, for thinking of the resources and expertise of his IT colleagues in the heat of the moment, and the second, for so effectively and dramatically illustrating a concern that is so much in discussion today—the ambivalence and lack

Related Posts

Cyber Security: The Cornerstone of IIoT Adoption

August 16th, 2017

of understanding that can exist between OT and IT colleagues.

Moving towards a new era of cooperation

As industry works – with varying degrees of success – to create a new world of IT/OT convergence and partnership, with the previously distinct lines and silos between the roles and responsibilities of each becoming more blurred, it pays to keep the comments of the Ukrainian operators in mind. If there had been greater teamwork between OT and IT in the plant in the months preceding, might the attack have been avoided or been mitigated in some way?

Whether or not that would have been the case, there are, unfortunately, more and more opportunities to ask the question. There has been a sharp increase in cyber attacks against industrial control systems, including a recent one that targeted plant safety instrumentation systems in the oil and gas industry. It's a disturbing increase in the level of maliciousness to think that human life could be targeted and not just equipment. Another frightening portent of possible things to come relates to a recent technical alert sent out by the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). CERT warned that a hacked schematic of an 8.8 megawatt turbine belonging to an American power plant was retrieved from a Russian command and control server. Conjecturing what that could mean is a very scary exercise. (However, on the positive side, getting forewarned with this information is the first step towards being forearmed, so it's a good opportunity for me to reiterate that if you are not yet subscribing to the outstanding alerts, advisories, reports and other

Strengthening the Security Posture of Critical Energy Infrastructures – Conversation with EnergySec's New President Steve Parker

September 20th, 2016

Industrial Networking: 5 Steps to Benefitting from the IIoT

December 2nd, 2015

Topics

ICS Security

SCADA Security

Industrial Cyber Security

Industrial Security

PLC Security

Industrial Networking

IoT Security

Industrial Firewall

Industrial Network Security

Stuxnet

View More

invaluable resources from ICS-CERT, do so right now!)

In late 2017, Belden's Tripwire group once again teamed with SANS Institute on their annual survey of ICS and plant operations engineering professionals to help provide a little insight. Among the disturbing findings: nearly 70% of respondents—insiders all—consider the current threat to their systems to be high or severe/critical. Their biggest single concern, they report, are devices unable to protect themselves being added to the network. A top attack concern is ransomware, which is exploding, with levels nearly doubling year over year. This is the environment that we are in today.

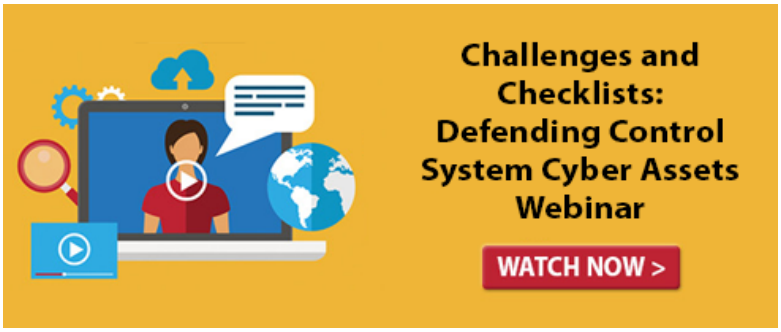
Leverage the expertise on the other side of the house

While we at Tripwire and Belden have many OT clients with fairly sophisticated cyber security resources, I believe that certainly, for the vast majority of organizations, the bulk of cyber security expertise resides in the IT department. After all, they have been doing it far longer than their OT colleagues and have been building expertise and organizational infrastructure over decades. And that's good news—it means that OT doesn't need to reinvent the wheel and build a new organization from scratch. Instead, they simply need to bridge the gap between IT and OT to accelerate their ability to ward off escalating threats and continue bolstering their cyber security.

IT has plenty to learn from OT as well. OT's earned expertise in prioritizing uptime and resiliency can no doubt find applications in other areas of the organization, as can their unrelenting focus on safety. Safety, of course, had never before been a driving priority in the IT world, but it's something that will need to become more pronounced as the silos between IT and OT inevitably crumble.

So how can OT and IT pros ease the transition? In a perfect world, of course, the drivers will come from senior management, who create the structure of the organization and codify expectations in formal policy and procedure "bibles" as well as in directions to their staff. But more informally, each of us can work to get to know colleagues on the other side of the "T" and reach out to them for relevant advice, never forgetting that there is a vital human element to the IT/OT convergence as well as a technological one. Maybe ask OT or IT managers to set up joint meetings focusing upon common goals. If appropriate, perhaps even ask for an embedded colleague; for example, an IT cyber security expert on full- or part-time loan to help with OT challenges. All organizations are different of course, but the OT/IT convergence will no doubt be looked back upon as a turning point in industry's fight for cyber security and further harnessing of technology for business success. Being an early, proactive leader in that regard certainly, in general, seems like a good role to be playing.

For a look at some other cyber security trends and business challenges, view our on-demand webinar **Challenges and Checklists: Defending Control System Cyber Assets**.



We at Belden and Tripwire work with a lot of different organizations in varying stages along the IT/OT

convergence continuum. We might be able to provide insight to issues you may be having. Call us and we'll be glad to start a dialog.

Related Links

- Blog: 70 Percent of Energy Security Pros Fear Digital Attacks
- Blog: How Plant Operators Can Overcome the Language Barrier to Securing OT Environments
- Blog: The Human Attack Surface: The Weakest Link in Your ICS Security
- White Paper: Network Security
- eBook: Industrial Cyber Security for Dummies

PREVIOUS POST
70 Percent of Energy Security Pros Fear Digital Attacks Could Produce a "Catastrophic Failure"

Robert Landavazo

Robert Landavazo is a Systems Engineer at Tripwire where he focuses on helping customers secure their Industrial Control Systems. He has a background in in the electric utility sector, most recently working to implement a NERC Critical Infrastructure Protection (CIP) internal compliance program leveraging Tripwire's own product suite. While at this utility, Robert worked in Operations Technology to support SCADA in Distribution, Transmission and Generation. Prior to his tenure in utilities, Robert worked in Public Safety, managing emergency communications infrastructure like Next Generation 911, IP Radio and Computer Aided Dispatch systems.

Comments

First Name*

Last Name

Email*

Website

Comment*

Subscribe to follow-up comments for this post

Yes, I would like to receive marketing information from Belden Inc. and its affiliates, subsidiary companies and brands indicated below. I therefore provide my consent to the use of the personal information submitted here for the purpose of providing me marketing information related to Belden and its subsidiaries' products, services and marketing events. I understand that I may withdraw my consent at any time.
Belden Inc. affiliates, subsidiary companies and brands include: Alpha Wire; Belden Deutschland GmbH; Coast Wire & Tech; Hirschmann Automation and Control GmbH; GarrettCom; Grass Valley; Lumberg Automation, Poliron; PPC Broadband; ProSoft Technology; S-A-M (Snell Advanced Media); Softel Ltd.; Thinklogical; Tofino Security; Tripwire; and West Penn Wire.

Additional information regarding Belden's data privacy policies, including how to withdraw consent, is available at Belden.com/about/privacy.

By clicking subscribe below, you consent to allow www.belden.com to store and process the personal information submitted above to provide you the content requested.

Submit Comment

