Securing the Future of Digital Manufacturing – Cybersecurity Considerations in an Era of Industry 4.0

written by Lauri Moon | February 3, 2020

In today's connected world, manufacturers are embracing automation and the Internet of Things (IoT) or the Industrial Internet of Things (IIoT) for competitive advantage. The merging of the cyber and physical worlds means improved efficiency, but it also means exposing your critical manufacturing infrastructure to cyber risk. In fact, according to an independent ICS study, nearly 6 in 10 organizations using SCADA or ICS industrial control systems have experienced a breach in those systems in the past year.

From IP-related tasks such as research, design and prototyping through to connected processes such as production, distribution and delivery, legacy and modern manufacturing systems – once protected by an air gap – are now connected to the network. The need for end-to-end security is greater than ever.

Listen in to this lively discussion from a panel cybersecurity experts and thought leaders as they break down the top trends impacting today's manufacturers security strategy, including IT and OT convergence, connected intelligent manufacturing and workforce dynamics.

In light of Industry 4.0, we'll examine three key ingredients needed in your cybersecurity strategy – visibility, control, and situational awareness – and their impact on the future of digital manufacturing.

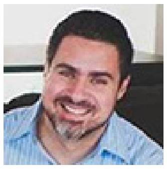
Speakers

Richard K. Peters (Rick), CISO, Operational Technology North America, Fortinet

Rick Peters brings the Fortinet OT-CI team more than 37 years of cybersecurity and global partnering experience working across foreign, domestic, and commercial industry sectors at the National Security Agency (NSA). As Fortinet's Operational Technology North American CISO, he delivers cybersecurity defense solutions and insights for the OT/ICS/SCADA critical infrastructure environments. Prior to Fortinet, Rick led development of cyber capability across Endpoint, Infrastructure, and Industrial Control System technologies at the agency. Previously, Rick also served as an executive leader supporting the Information Assurance Directorate at the NSA. Earlier in his career, he served in a broad range of leadership and Engineering roles including Chief of Staff for the NSA Cyber Task Force and a 5-year forward liaison charged with directing integration of cyber and cryptologic solutions for U.S. Air Force Europe, Ramstein AFB, Germany.

Don Rogers, Manufacturing Industry Practice Lead, World Wide Technology

Don Rogers leads the Manufacturing Industry Practice for World Wide Technology (WWT). WWT is a global consulting and technology organization with revenues in excess of $11B. WWT's vision is to be the best technology integrator in the world, by engaging consultatively "from Idea to Outcome" and aligning technology solutions with the vision, mission, strategy and business needs of its customers. WWT's Manufacturing Industry Practice is built "from industry, for industry" and is focused on making the "Digital Factory" and the "Industrial Internet of Things" a reality for manufacturers in various industry segments, including Food & Beverage, Automotive, Consumer Packaged Goods and Pharmaceuticals.



Enrique Martinez, Technical Solutions Architect, Industrial Control Systems Security, World Wide Technology

Enrique Martinez is a Technical Solutions Architect for Industrial Control Systems Security at World Wide Technology (WWT). In his current role, he helps customers with the selection and implementation of security tools for their ICS/OT/IoT environments, as well as develop long term security strategy. Enrique has 20+ years of experience in the cybersecurity areas of vulnerability management, intrusion detection, security architecture, compliance, and critical infrastructure protection in the financial and utilities sector. He spent 10 years leading the development of cybersecurity programs for generation (nuclear and fossil), transmission, and distribution.

Register

By clicking above, I acknowledge and agree to Informa's Terms of Service and to Informa's use of my contact information to communicate with me about offerings by Informa, its brands, affiliates and/or third-party partners, consistent with Informa's Privacy Policy. In addition, I understand that my personal information will be shared with any sponsor(s) of the resource, so they can contact me directly about their products or services. Please refer to the privacy policies of such sponsor(s) for more details on how your information will be used by them.