2015 Cybersecurity Day

Featured Speaker:
Moving Beyond IT\OT Security to a Strategic Security Program
Dr. Jerald Dawkins
CEO and Founder, True Digital Security, Inc.
Developing a culture of security within an organization is one of the greatest challenges for information security professionals. Effectively managing cross-organizational security change from Operational Technology (OT) to Information Technology (IT) and garnering executive buy-in are critical to establishing this culture and implementing a successful security program. This presentation will take a strategic look at implementing a sound security program that focuses on the business' operations while engaging industry standards and best practices, such as the Cyber Security Framework (CSF) or the Cybersecurity Capability Maturity Model (C2M2) as guides.

Panel Discussion:
Moderator: Blake Larsen, Western Refining Company

"Emerging Roles in IT/OT"
Dan Scali, Mandiant, A FireEye Company
Marc Westbrock, Koch Industries
The panel will discuss the silo mentality between ICS and IT personnel in a plant environment and why today it is more important than ever to do away with the "silo mentalities" and work together.

Presentation Sessions:
Cybersecurity Defenses in Refining/Petrochemicals in 2015

Cyberthreats and Subcontractors…Could You Be the Next "Target?"
Paul Plauche, Turner Industries
Cyber threat actors usually leverage the weak points in an IT security program. In the Target® breach, it was one of their subcontractors. With the proliferation of subcontractors in the industrial space, this presentation will address things to consider for IT security and intellectual property protection.

Analysis of the Capabilities of Cybersecurity Defenses
Michael Firstenberg, Waterfall Security Solutions
The threats to our critical infrastructure continue to evolve. As new cyberattacks are created and discovered, it is incumbent upon us to evaluate the capabilities of our defensive strategies and technologies against these new offensives.

This session will analyze standard information security defense technologies including anti-virus, firewalls, intrusion detection and prevention systems, encryption, patch management, vulnerability scanning, along with directive measures such as risk management and security awareness training for their effectiveness in preventing cyberattacks on critical infrastructure.

2015 Cybersecurity Day

Industrial Control Systems Cybersecurity

Cybersecurity Monitoring of an Industrial Control System
Terry Crain, Tesoro Corporation
This presentation will discuss SIEM devices that help with the gathering of events from computers, firewalls, and network devices, yet, require configuration to obtain useful information about cybersecurity issues.

Energy Sector Collaborative Opportunities in ICS Incident Management
Frederick Hintermister, NERC
The opportunity space for improved energy sector ICS incident response includes people, process, and technology dimensions. This conversation provides a focused look at where some of the most attainable and sustainable areas are to deliver better critical infrastructure resilience value and make a strong impact for the sector.

Configuring and Maintaining an ICS Security Architecture
Terry Crain, Tesoro Corporation
The intent of this presentation is to provide an overview of the design, successes, and monitoring of our Standard Security Architecture (SSA) at Tesoro Refining. Information security architecture is a critically growing skill set that we need in Industrial Control Systems. ICS networks need to allow communication between a defined set of devices that are rarely together on the same network. This includes communications with a business network which has many more computers, people, communications, the Internet, and subsequently, potential malware.

The basics of a defense-in-depth zoned network design begins with creating network zones of devices with similar objectives and functionality, as well as using network firewalls to limit the possible risky communications between zones and devices. The Zoned and Layered design allows added protection depths which help prevent critical ICS attached devices from being exposed directly to more vulnerable devices.

Cybersecurity & Procurement

Improving Credit Capture of Model Predictive Control by Strengthening its Link to Real-Time Optimization Using Synergizer
Paul Forney, Schneider Electric

In the digital world it is not possible to perform a visual inspection of an industrial control system to determine the quality attribute of "security". Hidden behind the fancy graphics and industrial trappings there may be lurking opportunities for mal-actors to insert their own brand of control over your facility, take what they want and leave the rest for their friends in the underworld to devour. Today's asset owners must arm themselves with new tools that fit with the problems of today and those yet undiscovered of tomorrow. ISA in collaboration with IEC has been in the process of working with industry experts to create the set of industrial cyber security standards, ISA/IEC 62443 as a basis for the measurement of this quality attribute.

2015 Cybersecurity Day

The Myth of "Secure Out of the Box"
Neil Peterson, Emerson Process Management
Customers expect vendors to supply their Industrial Control Systems as "secure out of the box". Industrial Control Systems have a significant number of built-in security capabilities plus additional services that can be implemented and configured based on security requirements of the asset owner. This presentation will provide insight into what is required from each party to get a system properly secured based on the risk environment of the system.