ABSTRACT for the 2016 ISA WWAC Symposium

Cybersecurity – Going Beyond Protection

Don Dickinson*

Phoenix Contact USA, Harrisburg, PA
(*Email: ddickinson@phoenixcon.com and Phone: 717-944-1300, ext.3868)

SUBMISSION TYPE

30 minute presentation

KEYWORDS

Critical Infrastructure, Cybersecurity, Industrial Automation and Control Systems (IACS), International Society of Automation (ISA), ISA/IEC-62443, ISA-99, NIST Cybersecurity Framework (CSF)

ABSTRACT

2015 was another banner year for security breaches. In addition to the countless cyber-attacks that occur daily there were numerous breaches that were significant because of the number of people affected and the type of data that was accessed or compromised. One of the more notable breaches of 2015 was the theft of highly detailed personal information – including fingerprints – for 22 million current and former federal employees from the U.S. government's Office of Personnel Management. 2015 also saw the largest theft of medical records to date as the result of attacks on two major health insurers, Premera and Anthem.

Cyber-attacks aren't limited to theft of personal information or financial records. Attacks on SCADA systems are increasing as well. According to the 2015 Dell Security Annual Threat Report, attacks on SCADA systems globally doubled in 2014 compared to 2013 and it is expected that the number of attacks will continue to grow dramatically. No one would dispute the need for a security plan to protect the control and SCADA systems that operate critical infrastructure. However, it is important to note that the even the most secure systems can be and have been compromised. Although protection from a cyber-attack is the first order of business, a utility must plan and prepare its response to a cyber-event. Having a comprehensive security plan increases the utility's resiliency, and ensures the availability and reliability of critical water systems.

In February 2014 the National Institute of Standards and Technology (NIST) issued the Framework for Improving Critical Infrastructure Cybersecurity to help organizations manage cyber risks within the critical infrastructure sectors, including Water and Wastewater Systems. A key part of the Cybersecurity Framework is the Framework Core. The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references common across all critical infrastructure sectors that are segmented into five functions: Identify, Protect, Detect, Respond, and Recover. These functions organize basic cybersecurity activities at their highest level. The Framework Core references key industry standards and best practices to provide specific guidance for each of the Core functions. One of the key standards referenced throughout the NIST Framework is ISA-62443-2-1: Establishing an Industrial Automation and Control Systems Security Program.

The presentation and paper, "Cybersecurity – Going Beyond Protection" will highlight how ISA-62443-2-1 provides valuable guidance for all functions defined in the Framework Core, not just protection. As such, ISA-62443-2-1 provides guidance for the development and implementation of a comprehensive, utility-wide cybersecurity plan.

ABOUT THE AUTHORS

Don Dickinson *has more than 30 years of sales, marketing and product application experience in Industrial Controls and Automation, involving a wide range of products and technologies in various industry segments. Don is the Senior Business Development Manager for Water Management, Phoenix Contact USA. He is a past chair of the NC AWWA-WEA Automation Committee and the current chair of the Automation Committee's Security subcommittee.*