ABSTRACT for the 2015 ISA WWAC Symposium

First – Make a Business Case for Cybersecurity

Don Dickinson[1]*

[1] Phoenix Contact USA, Harrisburg, PA

(*correspondence: ddickinson@phoenixcon.com and Phone: 717-944-1300, ext. 3868)

SUBMISSION TYPE

6-12 page paper plus 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

2014 was a banner year for cyber attacks. The attack on Sony Pictures in November was only the latest in a long string of high profile attacks with significant economic impact and even political ramifications. Further, cyber attacks are likely to increase, according to a recent survey by the Pew Research Center. As the report notes, "The Internet has become so integral to economic and national life that government, business, and individual users are targets for ever-more frequent and threatening attacks."

In addition to the current cyber threat environment, there is growing awareness of an even greater concern – the potential for a cyber attack on critical infrastructure within the United States. The national and economic security of the United States is dependent on the reliable functioning of critical infrastructure. In February 2014 the National Institute of Standards and Technology (NIST) issued the *Framework for Improving Critical Infrastructure Cybersecurity*. The purpose of the Framework is to help organizations manage cybersecurity risks in a cost-effective way based on the business needs of the critical infrastructure sectors, including Water and Wastewater Systems.

One of the key standards referenced in the NIST Framework is *ISA-62443-2-1: Establishing an Industrial Automation and Control Systems Security Program*. The target audience for this standard is the asset owners and operators responsible for establishing and managing a utility's cybersecurity program. Unlike other security standards that cover only technical considerations for cybersecurity, ISA-62443-2-1 focuses on the critical elements of a security plan relating to policies, procedures, practices and personnel. As such, it is a valuable resource to management for establishing, implementing and maintaining a utility-wide security plan.

The first step in developing an IACS security program as defined by ISA-62443-2-1 is Risk Analysis, starting with the business rationale for cybersecurity. As noted in the standard, "Establishing a business rationale is essential for an organization to maintain management buy-in to an appropriate level of investment for the IACS cyber security program."

The presentation and paper, "First – Make A Business Case for Cybersecurity" will emphasize the necessity of a business case as defined in ISA-62443-2-1 that justifies the commitment of resources needed to

manage cyber risks for a water or wastewater utility. Additionally, an overview of the NIST Framework will be provided.

ABOUT THE AUTHORS

Don Dickinson *has a BSEE from North Carolina State University. He 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 past chair of the NC AWWA-WEA Automation Committee and the current chair of the Automation Committee's security subcommittee. He is currently an AWWA Project Advisory Committee member for development of Process Control System Security Guidance for the Water Sector. Don has delivered numerous papers and presentations at industry conferences and events including AWWA and ISA primarily on the topic of cybersecurity for Industrial Automation and Control Systems. Contact: ddickinson@phoenixcon.com.*