ABSTRACT for the 2017 ISA WWAC Symposium

LESSONS FROM THE UKRAINE CYBERATTACKS

Protecting critical infrastructure against the new cyberattacks

Michael H Firstenberg *

[1]Waterfall Security Solutions, 20130 Lakeview Center Plaza, Suite 400
Ashburn, VA 20147
(*Email: michaelf@waterfall-security.com and Phone: 609-304-5715)

SUBMISSION TYPE

30 minute presentation

KEYWORDS

Cybersecurity, Risk, Cyberattack, SCADA, Security

ABSTRACT

What happened in the Ukraine can happen in North America, and indeed almost anywhere. This new attack methodology is not constrained to power distribution, but can be used to bring down any critical infrastructure operation. Some point to regulations and say "no, CIP will protect us" but this is simply not true. Others say "we need more or better intrusion detection" but intrusion alerts while the attacker turns off pumps is too little, too late. Similar discussions have been followed the situations such as the German Steel Mill attack, the Korean Nuclear attack, the French undersea cable attack, and many others.

We can no longer dismiss cyber-physical attacks as conjecture. We cannot continue to operate believing that the security offered by baseline compliance, roadmaps, and association guidance will be sufficient to protect our processes and keep our employees and customers safe. We must not make the mistake of employing directives and technologies that are intended to protect data when we look to protect our physical processes. Looking at cyber security the wrong way yields nonsense. We need to start asking better questions.

ABOUT THE AUTHORS

Mike Firstenberg, GICSP, GCIH, CISSP *is the Director of Industrial Security for Waterfall Security. Mike brings almost two decades of experience in Control System Security. The former chair of the American Water SCADA Council, Mike studied Computer Science, Chemical Engineering, and Mathematics at the University of Pennsylvania, and is an active participant in the ISA, AWWA, and AIChE. Contact: michaelf@waterfall-security.com*