

TOWN HALL

APRIL 27, 2011 AUSTIN, TEXAS



Obstacles to Information Sharing in the Electric Sector

Post Event Overview

Bill Bryan, Deputy Assistant Secretary of Infrastructure Security & Energy Restoration for the US Dept. of Energy, kicked off the discussion by saying “the government has only two solutions to all problems. We can either legislate or regulate. Unfortunately, security is an art – and you cannot legislate art.” Mr. Bryan postulated that the solution must be one of shared responsibility between industry and government.

Defining the Obstacles

The group discussed a number of obstacles they face when trying to share information with other electric sector participants.

We Are Not Speaking the Same Language

“We all want to be secure. But how do we get there if we don’t speak the same language?”

There was quick agreement that an acute need exists for a common security lexicon to help address the problem. IT

security people must learn the language of operations and vice-versa. There is little value in sharing information if neither group understands what the other side has to offer.

Cost of Improving System Security

Though some vulnerability information is shared between security researchers and control system vendors, many of the existing control system applications are still based on older operating platforms and lack

appropriate security controls. Vendors cannot afford to rewrite the code for their SCADA systems software, often citing that the cost of

upgrading cannot be recovered through the small market share. Further, utilities are generally unwilling to bear the cost of upgrading. Public

utility commissions cap profits, which forces utilities to “do more with less”. These cost barriers drive a general sense of apathy around sharing the information necessary to fix software bugs.

“Control systems people wear hard hats and steel toe boots and build systems that last 30 years. That blows the mind of IT people.”

Regulatory Issues

A number of attendees cited fear of the North American Electric Reliability Corporation (NERC) as the number one reason why they weren’t sharing information. Asset owners believed if they shared information, even with other asset owners, it might somehow get back to NERC and a fine would result. There was a clear concern that NERC, in their

“If the NERC standards were performance based everyone would talk to everyone. Since they are fine based no one talks to anyone.”

regulatory capacity, has to act upon information they receive which could potentially be a compliance violation.

Existing Views and Bias

Moderator Brandon Dunlap identified early in the discussion that, while we are advancing and becoming more

sophisticated in meeting security challenges, we often still look at the world through a “straw” which makes us a threat to our own success. Living with such a narrow view of the world will almost certainly lead to failure. It is critical that we learn from the successes of others. Likely we are not as different and special as we think we are. There are lessons to be learned from successes in other sectors.

Contractual Confidentiality

Often the contractual arrangements prohibit the sharing of information with others. An example provided was the work of a national lab which found a number of vulnerabilities in a vendor software product. Even though the asset owner was privy to the information they were contractually prohibited from sharing it. This led into a discussion about some of the work being done using open source technology platforms.

Inconsistencies in Document Protection

There is no common system for determining how to classify and protect information. For this reason practices vary dramatically between organizations. A document that is protected at one company may be considered public information at another. The laws regarding public information are vastly different between public and private companies as well. This lack of consistency makes information sharing very difficult. Attendees suggested that perhaps the Department of Energy could help provide guidance on the consistent protection of information. A related concern was the tendency by government to over-classify information

which also inhibits information sharing. Over classifying information often happens in the absence of clear guidance.

Lack of Vendor Certification

Some participants felt that there is a need to have a program that could provide a rating and approval system to vendor products. One suggestion was to model the program after the “Energy Star” program used to indicate the efficiency of home appliances. The term “Cyber Star” was offered. This topic was hotly debated among the group. In general, the group agreed that the concept was a good one but the implementation of such a program would be fraught with difficulty.

Tools to Measure Success

Measuring security was a topic that brought out some strong emotion. Attendees agreed that one of the obstacles in front them is the lack of a clear way to measure the success of their efforts. Without consistent criteria for measuring success it is difficult to get programs funded adequately and difficult to accurately share information with others. The group agreed that absence of an attack is not necessarily proof of success.

Summaries

Moderator Brandon Dunlap asked this question “*Is the reason you are not sharing information because of NERC and the fear of fines?*” He received a resounding “yes” from the asset owners in the room. Then putting the group on point, he reminded them that NERC fines are fairly new. We were not sharing information before fines became a concern so perhaps NERC is not as much of a factor as we like to think.

“the benefit of open source is not the technology but rather the community and the open sharing of information.”

“my PhD in business says that if it can't be measured it won't be funded.”

He also acknowledged that some problems don't have immediate answers. "The vendor security architecture problem is not going away any time soon because the solution to this problem is cost prohibitive. We are simply going to have to find ways to deal with this problem for now."

Patrick Miller, CEO of EnergySec and Principal Investigator of the National Electric Sector Cybersecurity Organization, gave a call to action for the four groups represented in the room which he referred to as the "legs of a table" Each table leg must be equally strong or the table will not support our goals. He challenged **Vendors** to not just sell security products to us but rather to build, develop, and sell *secure* products. He made it clear to **Asset Owners** that it is time to get over the fear

"the solution costs you \$2. Buy a cup of coffee, listen intently, and build a relationship."

and start building trusting relationships with each other. **Government** attendees were asked to engage in a "two-way street" of information sharing and deal with the issue of over classification. To

Academia he acknowledged that we do need theoretical work to see future possibilities but we need to shift some of the dollars into developing practical solutions we can use right now.

Conclusions

Based on the discussions of the day, the group was able to draw some basic conclusions. People are afraid to share information for a variety of reasons. Thus they need vehicles for sharing information that help to alleviate that fear. The group agreed that the "brokered" information arrangements that ICS-CERT and EnergySec both offer works well. Each group provides anonymity for those

sharing information so the fear of fines is less of a concern. The group agreed that making better use of these protected information sharing vehicles is a start.

Closing Thoughts

Patrick Miller said in closing "This is not about technology, it is about people. The only way to move forward with the existing systems that we have is to do it together. We already know that the bad guys are sharing the info – are you?"

Thank you to our Presenters and Panelists

William Bryan (Keynote)
US Department of Energy

Brandon Dunlap (Moderator)
Brightfly

Chris Blask (Panelist)
Alien vault

Deborah Bryant (Panelist)
Oregon State Univ. Open Source Lab

James Grimshaw (Panelist)
CPS Energy

Maarten Van Horenbeeck (Panelist)
Microsoft Security Response Center

The next NESCO Town Hall will be held on August 17, 2011 in Bellevue, WA. We will be discussing ways to measure security and success. See www.energysec.org/NESCO for more details.