ENERGYSECCONNECTED

News From the EnergySec Community

Nov/Dec 2016

In this Issue:

President'sReport

Holiday Greetings

Year in Review

As 2016 draws to a close, I'd like to recap a few of the highlights from this past year and look forward to what's coming in 2017.

2016 was an interesting year in the electric industry. The year's opening act was revelations about the attack in Ukraine, followed closely by the approval of version 6 of the CIP standards and the race to July 1st, and then the FERC Supply Chain order in July. No doubt, 2017 will bring more change in the compliance arena, and likely more drama in the form of cyber attacks.

EnergySec had a year of slow but steady growth. We added two new professional education courses, the CIP Audit Workshop, and a CIP for Low Impact Entities course. We were also privileged to add three top-notch instructors to our faculty: Brent Castagnetto, former Manager of CIP Audits at WECC, Bryan Carr, former Senior CIP Auditor at WECC, and Leonard Chamberlain, former CIP Auditor at FERC. We also added another full-time member to our team, Andrew Zambrano.

In the event space, we hosted our 12th, and no doubt our best, annual summit at the amazing Disneyland Resort Hotel. We're looking forward to being back there again this year for lucky number 13 and hope you'll join us. We also extended our reach to the State of Hawaii, hosting a 2-day educational event in Honolulu, something we'll do again this February.

We also made progress in our workforce initiatives. In June, we presented at the NERC CIPC meeting, discussing our workforce plans with more than 50 attendees. In October, we hosted our first event focused on high school age students in partnership with INTERRUPT, a Worcester based non-profit that designed the event's curriculum and activities. In 2017, we'll add a week-long security education event built specifically for industry professionals.

In November, we announced the formation of an Industry Advisory Board consisting of senior security leadership from utilities across North America.

2016 was a good year, and we have even bigger plans for 2017. Stay tuned.

-SHP

RealityCheck

Empathy and Ethical Policy - Thoughts for Security

by Jack Whitsitt, Security Strategist, EnergySec

A few weeks ago, I traipsed up to New York to attend the first ever O'Reilly Security Conference in NYC (Full Disclosure: I was on the program committee) and I thoroughly enjoyed the entire experience. One of the things that stood out about the conference was that even in its intentional, conscious, focus on the "Defender" aspect of security, it still included quite a number of presentations on the human and softer aspects of security. There was one entire track on the human element and another (bridging business and security) that touched on many of the same concepts. Finally, it seems like folks are getting the picture: our problems are not substantially non-technical and we need to do more than just say "Security requires people!"

The foci and themes of these "soft talks" varied, but a common thread I heard (and perhaps this is my bias) was that not only is listening to others important to security, but hearing them and including them is as well. Hearing folks and including them in our tribe is not something we are always so good at, but security depends on it. Security is an attribute of our collective efforts to make sure the grid provides power to customers and to the nation. If our goal is not to provide power, security has no place. If we have a grid without security, we may not be able to provide power. Security, business, and operational goals are fundamentally intertwined and accomplishing them involves every single person at your organization and many outside of it. Without communication, we cannot work together, we cannot identify common, mutually supportive goals, and we cannot build a resilient environment that will neither do more or less than it should.

This kind of cooperation across traditional silos and perspectives requires empathy. Empathy requires understanding where someone else is coming from, what their goals and needs are, what their hang-ups are, and genuinely trying to support their needs in the business and the value they can provide. It requires the assumption that everyone is doing the best they can (even if we must plan for the exceptions).

Still, security, by its nature, must often take on a policing function within an organization and that function often puts us between a rock and a hard place. It forces us to ask questions like: How do we maintain a relationship and communication with those we must constrain? How do we constrain those from which our authority stems in the first place? Where is the balance between enforcing policy and doing the right thing?

Is there a sane way of approaching these types of problems? Has someone already dealt with this? It turns out someone has - in 19th century England – Sir Robert Peel.

I learned about Peel during my favorite talk at the O'Reilly conference – Security by Consent – given by a lawyer, Brendan O'Connor. In his talk, Brendan introduced us to the principles of ethical policing (or the concept of policing by consent) developed by Peel. It turns out that the idea of a police force was completely new at the time and it required some thought as to what the most effective relationship that force could have with the policed. To that end, Peel set out 9 principles that, if you read them carefully, say a lot about what kind of relationship we in security should have with the rest of the organization when we must fulfill a very similar role. They are very much worth some thought; I suspect they can help many organizations and the folks within them find more mutually supportive and successful security relationships.

About the Columnist

Jack Whitsitt, security strategist for EnergySec, brings a breadth of cyber security knowledge and thought leadership to any project. His unusual combination of hard technical, public/private partnership development, facilitation, and national risk management experience allow him to provide particular insight into and leadership of strategic organizational, sector, and national cyber security initiatives and educational endeavors.

A participant in the national critical infrastructure protection dialogue for seven years, Jack has provided regular advice, insight, and thought leadership to all levels of government and industry and has been responsible for several successful sector-level initiatives.

Mr. Whitsitt's experience and skill at developing and providing targeted training and education opportunities to a variety of audiences allows him to effectively communicate his knowledge and to positively affect behavior, culture, and outcomes within organizations.

CommunityReport

EnergySec's Industry Advisory Board

Senior security leaders to advise on key issues

On November 1, EnergySec announced the formation of a new industry advisory board comprised of senior energy sector technology and security leadership. The board, with its varied expertise representing organizations throughout North America, will advise EnergySec on key security issues affecting energy organizations. Steve Parker, EnergySec president states, "The input of industry leadership will help us set priorities for programs that serve our community. We have always enjoyed strong relationships with security staff and management within the energy sector, but this board reflects our growing connection with senior leadership."

The board will meet quarterly with EnergySec leadership. A full list of board members with biographies is available online at http://www.energysec.org/board-of-advisors/.

CIOs and CISOs Playing Together - Summit Presentation Review

Are CIOs and CISOs compatible?

by Brandon Workentin, EnergySec Staff

One of the great discussions at EnergySec's 12th Annual Security & Compliance Summit featured Rani Johnson and Tim Virtue of the Lower Colorado River Authority (LCRA). Tim is the Chief Information Security Officer (CISO) and Rani is the Chief Information Officer (CIO) of their organization. Tim started the discussion by talking about how he does not report through the IT department. Instead, he and Rani both report to the same boss, who would be called a Chief Operating Officer in most organizations. He said that this structure allows the organization to balance both business needs and security needs, without allowing one section to dominate the other.

They then discussed how they worked to remove silos between IT and OT, as well as silos between separate OT units they had between different business units. Tim talked about how, by breaking down those silos, they were able to get better visibility and management of the different units, especially those which are not in scope for NERC CIP regulations which were traditionally not as protected. LCRA decided, rather than hiring more IT guys, or more cybersecurity people, or more OT operators and train them on security (each having drawbacks), to create their Enterprise Cyber Technology Program, with the goal of cyber, IT, and OT working together to solve security problems. Rani then talked about how, since the advent of this program, there has been a change between how IT and OT talk to each other, where they are now more likely to have a discussion over how to solve problems.

Next, they discussed how this program has also led to people from one department being cross-trained in other areas, allowing them to make better decisions by being able to consider the viewpoints of their colleagues from different departments. As Tim said, "Day to day, we want to know what they do, and they know what we do."

EnergySec Webinars -Targeted to Industry Needs

A Review of our Recent Webinar Offerings

by Brandon Workentin, EnergySec Staff

EnergySec has a long tradition of producing quality webinars on topics important to the security and compliance efforts of the energy sector. We have two types of webinars: Education Series webinars and Solution Series webinars. An example of an Education Series webinar is our recent members-only webinar to discuss the proposed requirements surrounding low impact BES Cyber Systems which was held on November 4th. While this webinar was only available to our members to view or watch the replay, not all of our Education Series webinars are only for members. For example, a roundtable discussion featuring representatives from industry as well as a Threat Intelligence Researcher from Palo Alto Networks was *Grid Cyber Lockdown - Sizing Up the Emerging Ransomware Threat to Utilities Infrastructure*. This was a great webinar that included participants from three different utilities who discussed how the ransomware threat affected them and how organizations can prepare for and respond to ransomware attacks, as well as the threat intelligence researcher, who talked about current trends in ransomware malware.

For Solution Series webinars, EnergySec partners with a vendor to present a webinar on a topic or solution that is relevant to the energy sector. Many times, these webinars include industry participants, who discuss how they solve their security or compliance problems. For example, we partnered with ProtectWise to present a webinar *Empowering a Small Security Team to Act Proactively*, which featured Richie Field of Hoosier Energy discussing how his small utility, with a limited security budget, was still able to solve their security problems.

If you have an idea for a webinar you would like to see, or even better, participate in, please email info@energysec.org with your ideas.

Meet our Staff - Sean Maloney

Sean Maloney, Security Architect

Sean Maloney is a talented software developer and security technologist. He has been with EnergySec since 2012 and supports all of our technology systems and related initiatives. Previously, he worked at PacifiCorp where he was a primary developer and architect of several internal security tools.

Sean is an avid gardener and all-around handy man. He has been married to his wife, Vicky, for 25 years and has 3 sons. Sean is also a Navy veteran.

EnergySec Vendor Resource Center

A Call For Participation

By Andrew Zambrano, EnergySec Staff

How does your organization vet a new product or solution? Do you roll the dice with google results and take a leap of faith (and large sums of money) to try products out on a trial and error basis? Maybe you wonder what the guy around the block is using? Does his solution match the needs of your organization or just his own? With the current standards, and the new ones on the way, you are constantly reassessing your approach and equipment. Do you have the right products in place to ensure you meet the standards, and hopefully at the same time achieve good security? Of course, you could always consult with a firm. They may charge you more than the product itself to tell you what fits your needs! What am I getting at? The EnergySec Vendor Resource Center (VRC). We are setting a few goals in order to strengthen and support the industry:

1. Provide a very low cost comprehensive resource to help organizations identify security-related products and services that may be appropriate to their needs in well-defined areas (i.e. "Categories").
2. Provide a mechanism for feedback and polling of the products currently out there. We are asking for opinion related to what you think the industry is experiencing from various vendors (rather than about your company). This provides benefit to the entire energy community.
3. Offer a safe place for entities to view any industry specific products or solutions and to discuss them with their peers and if appropriate a more personalized vendor contact.

So how can you participate? There are a variety of ways and levels of input you can provide for us to make a valuable resource for everyone, including your organization. We strongly believe the VRC is a community driven project and we want you to help us mold our framework into your ideal resource. Like many other open source projects, this ensures it will be readily available to its viewers and editors. We envision three phases that you can help with, some of which are already well underway: conduct security category surveys to get industry opinion, continue building our product database with support from industry, and connect useful vendors with the decision makers. If you are an entity or a vendor, there are ways to participate in creating a tool that can really help.

If you would like more information on the VRC please visit vendors.energysec.org or if you would like to join the VRC today, please create your EnergySec Community account at community.energysec.org and check out the VRC under the resources tab. Help us make the VRC the best energy product consumer resource out there!

Welcome, New Members

We welcome the following organizations to the EnergySec Community

We are happy to welcome two new industry members this month:

Lower Colorado River Authority (LCRA)

LCRA provides a multitude of vital services to Texans, including delivering electricity, managing the water supply and environment of the lower Colorado River basin, providing public recreation areas, and supporting community development.

Intermountain Rural Electric Association (IREA).

IREA is a nonprofit electric distribution cooperative with more than 140,000 customers within a service territory covering approximately 5,000 square miles in central Colorado, and is the largest of Colorado's twenty-three electric distribution cooperatives.

We are happy to have these new members as part of our ever-growing list of community partners.

Organizational membership provides many benefits in areas such as professional education, services, and workforce development. If you would like more information on specific benefits, please contact us for our latest Programs and Services book.

Full information on membership is also available on our website, or email at membership@energysec.org

Upcoming Events

Registration is Open!

February 22-23, 2017
2nd Annual Hawaii Education Series
Waikiki Beach, Honolulu, Hawaii

WorkforceDevelopment

Security Education Week

Designed for Entry and Mid-level Staff

We've been talking about workforce issues for a long time, and over the past couple of years we have been aggressively planning and executing our workforce program initiatives. In May of 2017, we will launch another key aspect of these programs, a week-long educational event designed for early-to-mid career electric sector cybersecurity professionals.

This event will have three primary goals:

- Increase the level of industry relevant technical security knowledge of participants.
- Increase the understanding of security relevant operational aspects of the electric power industry.
- Grow strong inter-company relationships between security staffs at utilities throughout North America.

Although we won't be officially announcing this event until late January, we can provide some preliminary information now. The event will be held at the conference facilities at McKinney Roughs Nature Park near Austin, TX. The site is owned and managed by Lower Colorado River Authority (LCRA), a major public power entity in central Texas. LCRA is assisting with logistics for the event.

This event will be educational, with a variety of industry relevant topics presented, hands on workshops, and breakout sessions. The agenda is still in early development, but we plan to have content in these areas:

- Industrial Control System (ICS) security
- Electric industry operations and related security issues
- Security technologies with wide deployment in the industry
- Incident response, forensics, and threat hunting
- Site tours of nearby LCRA facilities

We are also planning a variety of networking and social events designed to build relationships within industry and strengthen the community of cybersecurity professionals in our sector.

We are currently in discussions with numerous potential instructors, as well as utilities, who are helping us form the agenda. We welcome additional input into this event, and would love to hear from you if your utility is interested in participating.

CyberWatch West

A Consortium to increase Cybersecurity Education

EnergySec is privileged to be a part of the ever-growing CyberWatch West community. CyberWatch West is a National Science Foundation regional center for cybersecurity education with more than 110 universities, colleges, high school, and educational organizations belonging to the consortium.

CyberWatch West (CWW) provides support to community colleges interested in developing a strong cybersecurity education program. CyberWatch West provides mentorship to faculty members within their scope who are developing their own cybersecurity courses as well as to programs seeking to receive the National Center of Academic Excellence in Information Assurance/Cybersecurity designation.

CyberWatch West also provides free curriculum resources, including downloadable materials for a new course in Critical Infrastructure Security and Resilience (CISR) as well as access to an online library of more than 60 video recordings of webinars, presentations and online classes on cybersecurity topics.

CyberWatch West provide travel support for faculty to attend cybersecurity-related conferences and professional development events. CWW also helps colleges access industry partners for their internship programs, for college workshops, and for speakers who can share real-life experiences in working in cybersecurity. CWW also supports industry events to build community and networking opportunities for regional faculty, students, and industry.

Whatcom Community College

Providing innovative cybersecurity education

Whatcom Community College (WCC) in Bellingham, Washington, is a driving force in the development of cybersecurity education through its direction and participation in CyberWatch West. WCC was among the first community colleges in the United States to earn the distinction of being a National Center of Academic Excellence in Information Assurance/Cyber Defense 2 year education (CAE2Y), which recognizes colleges that are models of education and training in the information assurance field with curriculum mapped to the NSA's latest requirements.

In August 2015, the National Science Foundation awarded two grants totaling $6.4 million to Whatcom Community College to expand its cybersecurity program. The investment reinforced the college's nationwide leadership in cybersecurity and its unique role focused on expanding training on high-tech security from Hawaii to Texas. The first grant is to help establish a national network of community colleges that meet exceptionally high cybersecurity and computing standards. The second grant directly funds the CyberWatch West program, one of only four advanced cybersecurity education centers in the nation certified by the NSF.

"Funding from the National Science Foundation acknowledges the exemplary and cutting-edge work being done by Whatcom's faculty and staff," WCC President Kathi Hiyane-Brown said. "The College is proud to be at the forefront of cybersecurity education and to be recognized for creating meaningful advances in the cybersecurity field."

Through the formation and direction of CyberWatch West, WCC has taken on a national role in supporting colleges across the nation with resources and expertise to dramatically enhance two-year cybersecurity programs, as well as to create four-year degree pathways.

Today, largely due to the dedicated work of Corrine Sande, Computer Information Systems program director, and the faculty of WCC, Whatcom offers two-year degrees in computer information systems and cybersecurity (with opportunities to transfer to regional universities) as well as certificates. WCC recently announced it will offer its first applied baccalaureate degree - a bachelor of applied science (BAS) in IT networking — in fall 2017. This degree is the only one of its kind in the northwest corner of Washington state. BAS graduates will be prepared to enter the workforce as network administrators and related job categories such as computer and information systems manager or computer network architect.

Whatcom is also active in the STEM education field, creating initiatives that engage students at a young age, such as its interactive STEM workshops directed towards middle school students where students and their parent/guardian can run lab experiments, interact with experts, and ask questions about college preparation.

For more information regarding Whatcom's CIS and cybersecurity programs, visit whatcom.edu/cis.

ProfessionalEducation

Reducing Cybersecurity Risk: Tactics and Strategies

Renamed and Redirected

Our Cybersecurity Frameworks course with Jack Whitsitt, a well-known speaker and collaborator for cybersecurity initiatives and educational endeavors, has been renamed to reflect its new focus on mitigating risk through the application and understanding of traditional cybersecurity frameworks. The class is interactive and provides opportunities for attendees to have open discussion regarding applying framework principles to their organizational needs. The course is offered on a limited basis for 2017 with the first workshop scheduled for Phoenix, Arizona, on January 25-26, 2017.

For more information or to schedule a workshop, contact us at education@energysec.org.

Professional Education Staff Profile - Leonard Chamberlain

Meet one of our NERC CIP Instructors

Leonard Chamberlain has over 17 years of experience in network engineering, information technology, and industrial control system security. He worked as a consultant for Entergy where he was involved in their NERC CIP program.

Leonard also worked as an Energy Industry Analyst for the Federal Energy Regulatory Commission (FERC) where he served as a technical lead on audits (both observational and FERC-led), network architecture reviews, investigations, and NERC notice of penalties teams.

2017 Schedule

A look ahead to next year

We are currently developing our course schedule for 2017.We will offer two formats for courses this year. In some cities, we will offer multiple courses in two concurrent tracks. In other cities we will offer a 5-day format including both our NERC CIP Bootcamp and our Audit Workshop running consecutively.This will allow individuals to take both courses the same week.

Registration is currently open for the following cities and dates:

- Phoenix, AZ | January 23-26
- Nashville,TN | Feb 20-24
- Atlanta, GA | April 17-20
- Kansas City, MO | June 12-15
- Portland, OR | July 17-21
- Hartford, CT | Sep18-22

Additional planned cities are:

- Austin,TX | Nov
- San Diego, CA | Dec

InformationSharing andAnalysis

We continue to monitor the progress and participate in the development of standards for Information Sharing and Analysis Organizations (ISAOs) by the ISAO Standards Organization (isao.org). EnergySec is now listed as an ISAO in their directory.We are working on new partnerships for 2017 and expect a few announcements early in the new year.

RSA ISAO Meeting

A chance to connect with your peers

EnergySec has been granted a 45-minute block of meeting space at the 2017 RSA Conference in San Francisco. Details are still in the works, but we will use the time to discuss collaboration efforts amongst our membership and vendor partners. If you plan to be at RSA this year, let us know and we'll keep you updated as plans are finalized.

NERC CIPC and Briefing

Keeping in touch with industry

EnergySec staff analysts, Brandon Workentin and Andrew Zambrano, will be attending the December CIPC meeting and associated security briefing. Our staff routinely attends industry events to stay in touch with issues affecting the industry and help provide information and insights to our membership. If you'll be at CIPC in December, be sure to say hello and introduce yourself to Brandon and Andrew.

LITTLE BOBBY
by Robert M. Lee and Jeff Haas
WHAT ARE YOUR TOP FIVE SECURITY GOALS?
WE'RE WAITING TO SEE NEXT YEAR'S BUDGET.
CISO
WHAT WAS THIS YEAR'S BUDGET?
FIVE BANANAS FROM THE BREAK ROOM.
CISO
MAYBE WE CAN HIRE SOMEONE LOW ON POTASSIUM.
CISO
HAAS