ENERGYSEC CONNECTED

News From the EnergySec Community

August 2016

In this Issue:

President's Report

Welcome

Introducing EnergySec Connected

Welcome. One of the things that's become obvious to me recently is that, although many people in the industry have heard of EnergySec, few really know all that we do. Honestly, sometimes it's hard for me to keep up with all we do, and are aspiring to do. That's the reason we are launching a new, monthly publication with news and stories from our community. We call it, EnergySec Connected.

EnergySec Connected will keep you up to date on events, activities, and other news from the EnergySec Community. You'll learn how your peers in the industry are tackling security challenges, working together on key issues, and meeting compliance obligations. And, you'll hear about EnergySec's efforts to support industry, grow the security workforce, foster community, and many other things.

One of the common challenges I hear about is the shortage of skilled cybersecurity professionals. This month, we feature two stories that portend positive change in that regard. First, you'll hear about a cyber bootcamp we were privileged to support this past month. Second, we'll discuss another high school level event that EnergySec is supporting. There's a great wave of cyber professionals rising up, if we can just encourage them, guide them, and most importantly, put them to work.

We'd like to hear from you. Do you have a story to share with your peers in the sector? Drop us a note at connected@energysec.org.

-SHP

RealityCheck

DNC and the Global InfoSec Conflict

by Jack Whitsitt, Security Strategist, EnergySec

For every news article about a new cyber "attack" or data dump, there is a subsequent outcry of "game changer! game changer!" Yet, it never feels as if the game has changed. This is because it hasn't and the DNC email event is a classic example of why: we are presently, and have been for some time, in the middle of large scale active global conflict online and each of us is a participant (whether we know or agree to it or not). There is nothing new here, the game is already in play.

Groups of people, with temporarily-aligned interests, are collaborating to exploit us, our nations, our businesses, and our institutions online to further their own goals.

The idea that there is anyone who is *not* part of this conflict is probably untrue, and more people would have an understanding of this if fewer folks didn't want to avoid acknowledging this reality.

First, if you are connected to the internet, that makes you *part* of the internet by definition; firewalls and laws are resistance barriers, at most.

Second, the internet is "the geography over which international conflict takes place" (there is evidence here as we will see monthly in these newsletters).

You are, therefore, definitionally a part of the international conflict.

That does not mean, however, that you are a defender. I find a siege to be the most appropriate conflict metaphor here (if a very flawed one): The environment in which you operate is subject to a sustained, intentional, resource draining conflict. You are not part of the military, yet your actions are constrained by the overall conflict in general and, in some cases, there are effects specific to you. You can try and manage your own risk, but since the threats and vulnerabilities are largely systemic in the environment in which you operate, you can, at most, delay some of the particular effects - you lack the resources and scope of influence on the entire environment to do more.

Using this siege analogy, strategic change requires substantial non-technical policy, legal policy, and cultural cooperation across entities of all types (civilian, industry, government, and military).

Further, because your infrastructure is shared (by virtue of being part of a larger "internet), and because your infrastructure is likely integrally reflective of your business (or identity, if you are an individual), *you yourself* are likely part of the conflict, not just your network and "cyber infrastructure".

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

12th Annual Security and Compliance Summit

This year may be the best ever

We are gearing up for our 12th annual Summit, being held this August 20-22 in Anaheim, CA. We have a great agenda lined up with speakers from several utilities, leading industry vendors, researchers, and the federal government. And we have a great venue!

This year we are bringing back the panel format that proved popular in our early years, and supplementing with keynotes and dynamic presentations. We'll have a recap of the event in our September issue.

New Members

We welcome the following organization that recently joined EnergySec.

We are happy to welcome three new members this month. Two new industry members, Los Angeles Department of Water and Power and Garland Power and Light. One commercial member that recently joined is WizNucleus, a maker of security and compliance solutions.

Organizational membership provides many benefits in various areas. Full information on membership is available on our website, or by contacting us at membership@energysec.org

Tracking The SDT

EnergySec follows the development of new CIP standards

At times, the world of NERC CIP can turn into a whirlwind of activity. No one understands that better than Kim Zimmerman, EnergySec's lead staff member for NERC CIP issues. Kim follows as many CIP related events and activities as possible, including the current NERC CIP drafting team efforts.

"One of the challenges in tracking activity on a national scale is the time zone difference. I've had many very early mornings catching an east coast conference call or webinar," notes Kim. But, her hard work pays off for EnergySec members who receive comprehensive updates on CIP events across the nation via our bi-weekly CIP Newsletter. "It's interesting to listen to the drafting team calls because you gain a lot of context and background on why the team went one direction or another with the standards," said Kim.

Kim's work also helps other staff members and leadership keep abreast of the changes and informs our work of developing comments on CIP standards and other relevant items.

Kim can be reached via email at kim.zimmerman@energysec.org, or (503) 850-0163

Volunteer Opportunities

Get Involved and give a little back

EnergySec offers many ways to get involved. One of the key areas where help is needed is in our workforce programs. We are building a speaker's bureau for individuals interested in speaking to local schools in their area about security careers in the energy sector. We are also seeking individuals interested in mentoring budding cybersecurity professionals, assisting with curriculum development, and serving on our workforce advisory group.

For more information on volunteer positions, visit our website at www.energysec.org/volunteer, or email us at volunteer@energysec.org.

Upcoming Events

August 20-22
12th Annual Security and Compliance Summit
Anaheim, CA

October 1
1NTERRUPT Cyber Event
Mt. Hood Community College, Gresham, OR

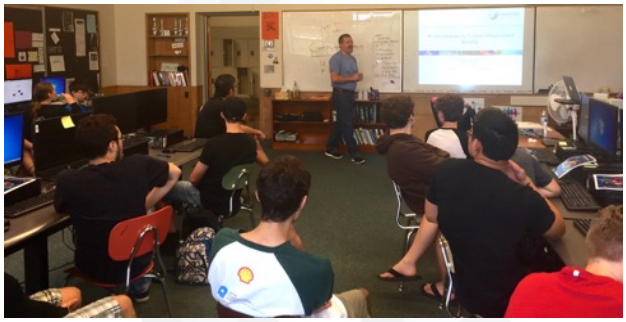
WorkforceDevelopment

Portland CyberPatriot Camp

Steve Parker discusses securing the power grid

EnergySec had the privilege to participate in the Portland Cyber Patriot Camp held at Lincoln High School in Portland, OR., from July 18-22nd. The camp was organized by Amelia Kawasaki (Lincoln High School Sophomore & Coding Club President), Zandar Work (Lake Oswego High Junior), and Charlie Kawasaki. (Software and Cybersecurity Entrepreneur).

The camp had 30 registered students who were required to have a teacher reference for participation.



The students who attended were highly motivated to learn new things, to accomplish the goals set, and to develop friendships with other students who were like-minded. The students worked in teams which supported students who may not have had as many diversified learning experiences as their teammates.

The cost of the camp was offset for the students by sponsors.hips from the local community. Several of the sponsors also participated as guest speakers at the camp, providing valuable insight into the varied workplaces of cybersecurity.

The Air Force Association's Cyber Patriot materials were used throughout the week as the ground work for completing the CyberPatriot challenge on Day 5 of the camp. The teams were challenged to complete the challenges with the most points.

The students and their families were given an opportunity to meet and mingle with some of the speakers and sponsors of the camp. Parents found this time rewarding as they saw their student "finding their niche" in the world of work and receiving information on career pathways for their student's future.

> *"I found the camp informational and definitely an eye-opener. I think being at this camp has inspired me to do more."*
>
> - Student Participant

"The camp was such a hit with the students, families and contributors that even though I told everyone it's a one-time event," wrote Charlie Kawasaki, "we've begun discussions with EnergySec to do it again next year. "

EnergySec, devoted to educating the next generation of cybersecurity professionals, has agreed to join with Charlie Kawasaki and the student organizers in the development of two PDX Cyber Summer Camps for 2017, one camp focusing on a "girls only" format and the second camp being co-ed.

INTERRUPT 2016

EnergySec directs Portland Chapter of INTERRUPT

EnergySec has been named as the Portland "chapter" of INTERRUPT, an organization focused on encouraging high school age students and young adults to consider careers in cybersecurity. We will be producing a 1-day event in Portland, OR, on October 1st targeting up to 50 students.

This effort is part of our larger plan to help grow the cybersecurity workforce in our industry over the long term. We are working to model programs in our area that can be scaled nationwide. If you're interested in organizing or participating in this or similar events in your area, drop us a note at workforcedev@energysec.org.

For more information about INTERRUPT, visit www.INTERRUPT.com.

ProfessionalEducation

NERC CIP Audit Workshop

A Review of EnergySec's Newest CIP Course

EnergySec launched its latest course offering this June in Oklahoma City. Dubbed the "NERC CIP Audit Workshop." The class is intended to educate participants on all aspects of CIP audits, including internal validation of compliance with the CIP standards.

The course begins with a look at FERC policies on enforcement, internal compliance programs, and penalties and sanctions. NERC Rules of Procedure, the Compliance Monitoring and Enforcement Program, and the Generally Accepted Government Audit Standards (GAGAS) are also covered. RSAWs and evidence requirements are discussed in depth from various perspectives.

Onsite Courses

We Deliver! Save time and money by bringing our courses to your location

All of our educational courses are available for onsite delivery. We can even customize the content and course length to meet your needs. If you have 10 or more individuals interested in a class, contact us to arrange an onsite course at a time and location convenient for you.

2017 Schedule

A look ahead to next year

We are currently developing our course schedule for 2017. We have two dates and locations finalized and registration will be opening soon for **Phoenix, AZ, in January** and **Nashville, TN, in late February**. Other cities planned for 2017 include:

- Atlanta, GA | April
- Kansas City, MO | June
- Portland, OR | July
- Boston, MA | Sep
- Austin, TX | Nov
- San Diego, CA | Dec

InformationSharing andAnalysis

EnergySec and Information Sharing

A Brief History of Information Sharing and Analysis Organizations (ISAOs)

Brandon Workentin, Security Analyst, EnergySec

The topic of "information sharing" has long been discussed, both at the policy level and at the down-in-the-weeds, analyst-to-analyst level, as a way for organizations to better defend themselves against cybersecurity threats. The federal government has been actively encouraging organizations to share more information and increase both public-private information sharing efforts as well as private-private information sharing. Perhaps the most high-profile example of these efforts was the Cybersecurity Information Sharing Act of 2015, which provided legal protections for organizations which shared cybersecurity information with the federal government.

However, that is not the only effort by the federal government to encourage information sharing. Executive Order 13691, released on February 13, 2015, called for the creation of Information Sharing and Analysis Organizations (ISAO). Both the White House and the Department of Homeland Security (DHS) have been actively engaged in the development of the ISAO framework,

EnergySec has served in an ISAO-like role since its inception, and is participating in the ISAO process to ensure we can continue to serve our members in that capacity as the role becomes more formal and better organized.

with DHS taking the initial lead and providing a grant to the "ISAO Standards Organization" (ISAO SO) to develop standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices.

The ISAO SO is using a public process to develop those standards and guidelines, including the use of ongoing public meetings as well as Working Groups involving industry and government stakeholders focused on the creation of ISAO standards. EnergySec's Brandon Workentin has been involved in some of these Working Groups, including the ISAO Creation and the Information Sharing Working groups. The initial standards are expected to be released in late-September, 2016. They will include what, in development, is called the "working tool," which provides guiding questions an ISAO can/should answer regarding how the ISAO will be formed, what the expectations of the members are, and what benefits the ISAO will provide to their members.

One part of the working tool focuses on the topic of trust. One of the key themes in the development of the ISAO standards is the need for trust between an ISAO and its members, as well as trust between separate members of the ISAO. As the size of information sharing organizations increases, there may be diminishing returns since the relationships upon which trust are built on become too numerous to be successful.

For example, a national organization with broad scope, such as the E-ISAC, provides benefits such as the capability to plan and coordinate activities on the scale of GridEx. However, an organization that is more focused may be able to attain higher levels of trust and interaction, with information being shared more quickly and in more detail due to the members familiarity with the sources of information provided to the community.

EnergySec has served in an ISAO-like role since its inception, and is participating in the ISAO process to ensure we can continue to serve our members in that capacity as the role becomes more formal and better organized. For more information on our ISAO efforts, contact us at isao@energysec.org, or call us at (503) 905-2920 (option 4).

Contact Us

We love hearing from our friends in the industry. If you have a question, comment, or simply want to learn more about one of our program areas, visit our website for more information, including contact information for all our staff.