ENERGYSECCONNECTED

News From the EnergySec Community

January 2017

In this Issue:

President'sReport

And We're Off…

Hitting the ground running in 2017

EnergySec's home city of Portland, OR, is suffering through one of its coldest winters on record, but fear not, our staff continues to work hard on our plans for 2017.

There are a few things I'd like to point out from this issue. First, plans are progressing well for our 13th annual Summit. We've made some tweaks to the agenda for this year, expanded our vendor expo, introduced focused tracks on day 1, and are debuting a student scholarship program designed to connect industry to future security professionals. More details on these topics are presented later in this newsletter.

This year, we are also debuting a new event we call, "Security Education Week." This will be a one-week event presenting industry-relevant security education designed for early to mid-career professionals working at electric utilities. The event will also feature evening activities designed to foster networking and to build relationships within industry. A formal announcement and draft agenda for this event is planned for early February.

Security Education Week is a big part of our workforce development program for 2017, but there's plenty more going on. We will once again host a high-school focused event, INTERRUPT, in Portland, and we are also supporting a week-long cyber camp for high-schoolers. We will also be ramping up our support for internships within industry, building out an apprenticeship program, and more.

Finally, we are working to expand our activities as an ISAO (Information Sharing and Analysis Organization), with a focus on services to our members. We'll be attending this year's RSA Conference and have been granted meeting space by the Conference to meet with our community. More on that appears later in the newsletter.

As always, we love to hear from our community about the work we are doing. Drop us a note anytime at info@energysec.org.

-SHP

RealityCheck

Risk and the FAIR Model Definition

by Jack Whitsitt, Security Strategist, EnergySec

In today's cybersecurity world, you've probably heard the word "risk" a lot; more than "a lot." In fact, the English translation of "Ad Nauseum" is usually understood to be: "so often it makes you as ill as hearing the term risk management".

Folks throw the word around like it's a penny. "Oops, I just dropped another use of 'risk' on the floor. Oh well. Leave it."

There are risk assessments, risk reports, big risks, little risks, cyber risks, managed risk, business risk, and on and on and on.

Mostly, no one uses the term in either a helpful or formally correct way (despite there being **several** formally correct uses to choose from) – and this is a problem, because you can't manage something you cant describe. You end up managing something else entirely – and usually leaving yourself much more exposed than you had intended.

For example, when folks say "risk", they often mean things like these instead:

- Vulnerability
- Bug
- Exposure
- Threat Actor
- Attack Vector
- Concern
- Fear
- Control Gap

None of these are risks – they are **pieces** of risks. Conceptually incomplete phrases as opposed to a complete risk sentence/description. If you're trying to manage "risk" and instead you're managing these, you have a huge problem on your hands that cannot even be **described** well enough to start fixing.

So what IS a risk? Is there a definition that is actually helpful and complete? Yes! The FAIR (Factor Analysis of Information Risk) model has maybe the most practically useful definition for classic Information Security Risk Analysis (which…allows…risk management):

"The probable frequency and magnitude of loss."

Wow, that's elegant and clear. Let's examine what makes it special:

1. It describes a probability, not a possibility. All things are possible, that doesn't mean they're going to happen. If your "risk" doesn't have an element of uncertainty in it, it isn't a risk.

2. It describes "risk" in terms of **loss**. If your "risk" doesn't describe a person or group who will experience loss, what that loss might be, or where that loss might come from, it is, again, not a risk – because in order for there to be a risk, someone must lose something. That is **literally** why it is a risk.

3. Magnitude – Attempting to describe "loss" without potential "magnitude" means you're not fully describing the loss. Without articulating loss, well, see #2.

4. Without "frequency", it's pretty hard to describe "probability", and if you can't describe probability, you're – again – either describing an actual loss without the "risk" component, or you're merely describing a possibility.

So how do we break this down into the type of information that a "risk" description might need in practice? Consider this statement:

"There is a RISK of one or more THREAT COMMUNITIES, whose actions may have one or more IMPACTS on one or more ASSETS at a FREQUENCY which could cost an ENTITY specific RESOURCES by exploiting one or more WEAKNESSES using an attack VECTOR unless effectively CONTROLLED."

Embedded in this one sentence are A) Many of the same terms we often improperly substitute for "risk" combined in a way that, B) Fully describes potential information security considerations that go into determining the probable frequency and magnitude of loss someone might experience.

Please, go forth, spread the word, and manage "Risk". You might consider looking into the "FAIR" analysis model along the way.

(Sincere apologies to those formalists who might take issue with any of the wording in this article, focusing on the importance of…wording).

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 13th Annual Security and Compliance Summit

Preview of this year's premiere event

This year, EnergySec will produce its 13th annual Security and Compliance Summit. We are looking forward to another successful event at the wonderful Disneyland Resort Hotel in Anaheim, CA. We are always looking for ways to improve and, to that end, we've made a few changes to this year's program that we'd like to tell you about.

First, on Day 1 of the Summit, we will be hosting special utility-only meeting tracks. These tracks will be open to utility personnel with job responsibilities in specific areas, including security leadership, security operations, and CIP compliance. The purpose of this is to facilitate more open sharing and networking amongst utility peer groups, provide more targeted content, and strengthen our community.

Second, we are offering an expanded vendor expo with double the space of last year's event. The expo hall will feature standard 10x10 and 10x20 booth layouts. We have also added dedicated expo time to the agenda to ensure that all attendees have a chance to explore the numerous products and services that will be on display.

Third, as we enter the fourth year of our security awards program, we are opening the nomination process. Previous award recipients have been selected by a small committee, but we'd like to expand the reach of this program and include more nominees for consideration. A nomination process will be announced and opened on March 6th for a 60-day nomination period.

And finally, we are very excited to announce a new program tied to our workforce development efforts. We plan to offer up to 50 Summit scholarships to outstanding college students interested in pursuing cybersecurity careers in our industry. This program will cover Summit attendance, lodging, meals, and one evening in the Disneyland Park. In addition, students and scholarship sponsors will be able to attend a special Monday evening dinner. This will enable both prospective employees and employers to interact and, hopefully, will lead to new professionals entering our industry.

Below are a few key dates related to the Summit:

Feb 6th	- Call for Speakers opens
March 6th	- Awards Nominations open
April 17th	- Registration opens
May 22nd	- Draft agenda posted
July 6th	- Final agenda posted
July 21	- Hotel room block ends
Aug 14-16	- 13th Annual Summit

CIPC and the Energy Sector Annual Classified Briefing

Quarterly Meeting Recap

by Brandon Workentin, EnergySec Staff

Brandon Workentin and Andrew Zambrano represented EnergySec at the CIPC meetings and annual classified briefing which took place in Atlanta, GA, in December. One interesting item to note from the classified briefing is that there was some discussion after the briefing about making the energy sector classified briefing a quarterly event, as opposed to annual. These discussions were in the very preliminary stages, but the idea involved using local Fusion Centers or FBI field offices to host a video conference. We are not aware of a contact person who is spearheading this effort, but talking to your contacts at NERC or your local Fusion Center may be worthwhile if this is something you would like to see happen.

The CIPC meeting was not ground-breaking, but there were also some interesting discussions. Somebody, my notes do not say who but from my memory it was possibly Marcus Sachs, talked about an electric utility which had a DDoS attack of 30-35 GBPS, which led to their ISP taking them offline. This affected the business side of the utility. Reading between the lines, this seemed to be the largest DDoS which had E-ISAC news, they said that 7-10 companies are in progress to do a STIX/TAXII pilot for the CRISP program.

Tobias Whitney, of NERC, talked about the recent Emerging Tech Roundtable which NERC hosted in November. He said that NERC would write a "value-add paper" to describe the operational and reliability benefits of using Cloud services, and industry examples of the use of them. He also said that there should be Implementation Guidance addressing how to obtain compliance evidence from cloud providers. Neither of those papers had a timeline given for them. This led to a bit of discussion about cloud services, virtualization, and compliance issues, with some comments along the lines of, "It seems like the auditors do not even know how to audit the current standard." In other NERC news, Scott Mix said that they expect the upcoming supply chain standard to have a 12-month implementation timeline. This would give utilities 12 months to design their programs, and then contracts after that 12 months are what would need to meet the standard.

One other topic which got a lot of discussion time was the use of Nuclear Regulatory Commission (NRC) background checks being sufficient for NERC CIP Personnel Risk Assessments (PRA). A group of utilities, which seemed to be led by Exelon Nuclear, had created a presentation showing that NRC checks were equivalent to, or more stringent than, PRA requirements. This did not seem to matter to some auditors who were present. The auditor did not want to rely on an attestation from NRC compliance people that somebody had received clearance, and the Nuclear people present were saying that wanting to see the personal information contained in an NRC background check would likely be a non-starter.

Hacking the Power Grid: Analyzing What Hackers Do When They Have Access to the "Power Grid Honeypot" - 12th Annual Summit Presentation Review

12th Annual Summit Presentation Review

by Brandon Workentin, EnergySec Staff

Dewan Chowdhury, of MalCrawler, closed last year's EnergySec Security & Compliance Summit by talking about the honeypot systems he has made to emulate Energy Management Systems (EMS). He described the honeypot, which includes power generators, transmission lines and substations, and distributed generation, such as solar. Chowdhury talked about how he is able to customize the honeypot, such as by changing the name and logo of the HMIs or changing the language of the text. This allows the honeypot to have, for example, an IP address and substation names which match the geolocation of that IP address.

He then started talking about what he has seen when people attempt to connect to the honeypots. He talked about how they open the honeypot up to attackers. One way was to open direct wifi access, like if a technician had installed a rogue access point. He said in that case, the "attackers" are typically people looking for free Internet access, and there was no real useful information gained. The next scenario was by using a "misconfigured" firewall which allows an attacker to pivot from IT to OT. He said that for the most part, once an attacker left their comfortable IT environment and started seeing OT protocols, such as DNP3, there wasn't much activity. The third way was to purposely open malware within the OT network, which Chowdhury said was the most effective way to see interesting attacks.

Chowdhury talked about what attackers do when they are on the system. He said that when attacks came from Russia or China, they generally followed an unwritten rule that espionage was okay, but sabotage wasn't. The attackers would try to collect information, but not try to turn the power off. He said it was different with the Middle East, where when they created an Israeli or Saudi company, the first thing that attackers did was try to sabotage operations. Chowdhury said that when it came to U.S.-based targets, the attackers went after things such as transmission diagrams and other intellectual property, rather than sabotage.

He finished by talking about technical lessons which can be learned from his research. He said that the first thing they recommend is looking for file system changes and file integrity, as well as looking for network traffic which is not normal, such as weird user agents or dns queries. He also gave other tips, such as making sure that you include Operations and Maintenance costs, i.e. people, whenever you buy a security tool, and to leverage the knowledge of the people who are running system protection systems, as, "They know the environment better than anybody else."

During the Q&A period, Chowdhury said that if you are in the industry, then the honeypot is free to use, and to contact him if you are interested in accessing the honeypot.

Meet our Staff - Brandon Workentin

Cybersecurity Analyst II

Brandon Workentin joined EnergySec as an intern in the Spring of 2014. He started with us as he was finishing up an Associates of Science in Cybersecurity and Networking at Mt. Hood Community College in Gresham, OR. Brandon has a background as a math and English teacher, and he put those skills to work by taking over responsibility for writing the Weekly Update as his first project at EnergySec.

After finishing his degree, Brandon became a full-time employee at EnergySec in August, 2014. Since that time, he's been focused on a wide range of activities for EnergySec. He continues to write the weekly newsletter, while also producing other content such as white papers, CIP commentary, and contributing to various webinars. Brandon also maintains the EnergySec websites and Twitter account. He occasionally travels to industry events where he enjoys meeting our members, especially if it's during happy hour.

Brandon has a lovely wife and four boys, ages 4, 5, 8, and 18. Most of his spare time is taken up with the boys, and he especially enjoys coaching their basketball teams, even though with the younger boys the game they play only vaguely resembles basketball.

Upcoming Events

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

WorkforceDevelopment

The Making of a Successful Internship

Five Areas to Consider for Your Summer Internships

It is the start of a new year — a good time to consider your internship needs for the spring and summer months. It is also a good time to evaluate the successfulness of your internship programs. Here are five areas to consider when reviewing your internship needs:

1. Can you provide the intern with legitimate projects which provide real work experience? Internships, whether paid or unpaid, need to provide the student with educational value to further their knowledge of the industry.
2. Are you prepared to provide adequate training throughout the internship? Be realistic about the kinds of information that your intern will or should know. Be ready to provide a "buddy" or partner for quick answers to keep the project moving.
3. Is the work to be done challenging? Does it make a difference? Interns are students who need to be challenged to continue their learning. They also want to know that the work matters to your organization.
4. Are you able to provide a good mentoring relationship for each intern? Mentors should be able to relate one-on-one to the intern in order to provide career guidance and reasonable goals.
5. Are there opportunities for interns to meet other professionals in your organization? Networking provides connections that interns need to continue to be active in the industry.

EnergySec is developing our internship program to help organizations identify possible candidates through our outreach to local colleges. We are also developing utility-specific education for interns and work models for organizations that can help identify real work experience projects that will be of value to both intern and company.

For more information, go to: www.energysec.org/workforce-development.

Scouting for Talent

EnergySec Member Benefit

Are you an EnergySec member? EnergySec's workforce development team is working on **your** behalf in **your** region. We are diligently pursuing contacts at major colleges, universities, and 2-year community colleges that are active in cybersecurity education. Our goal is to establish working relationships between these schools and our member organizations in the region who are looking to add or grow their internship program.

For more information on colleges in your area or to participate in our workforce programs, contact us at workforcedev@energysec.org

ProfessionalEducation

Hawaii Educational Series - A Sold-Out Event

Second Annual Event

Our second annual Hawaii Educational Series event to be held in Waikiki Beach, Honolulu,, HI, on February 22-23, is a "sold-out" event. Currently, we are expecting 65 attendees, including students and faculty from the University of Hawaii and BYU-Hawaii, Pacific Navy and Air Force, health organizations, and technical companies.

This two-day event focuses on mission critical security, covering topics such as "Reducing Cybersecurity Risk: Tactics and Strategies," taught by Jack Whitsitt, Senior Security Analyst for EnergySec, and "Let's Explore: NIST SP800-15 - Guide to Cyber Threat Information Sharing," taught by Leonard Chamberlain, Senior Security Consultant for the Archer Security Group.

With plenty of networking opportunities throughout the day, as well as a Welcome Reception the first night, this will be a premiere event for all those in attendance.

Professional Education Staff Profile - Wally Magda

Meet one of our NERC CIP Instructors

Wally Magda, an internationally recognized cyber and physical security expert for ICS, has many years of practical, hands-on, security experience which spans military command and control systems, intelligence agencies, and cyber/physical security enterprises. As a regional NERC CIP compliance auditor, Wally's professional tone demonstrated to all stakeholders the importance of adhering to the rules of procedure. He successfully completed 100 on- and off- site audits.

Currently, Wally focuses on teaching ICS cyber and physical security training courses as well as conducting cyber and physical security assessments for industry (i.e. electric energy, natural gas, water reclamation, manufacturing facilities).

Security Education Week

A utility focused, technical education event

We are working diligently to finalize the agenda for a unique new event planned for this May. Dubbed simply, "Security Education Week," this event is designed to build the technical security skills and industry knowledge of early to mid-career cybersecurity professionals working at electric utilities in North America.

The event will be held May 15-19 in Austin, TX at facilities of Lower Colorado River Authority (LCRA).

The agenda will feature 1/2 day deep learning sessions on utility-relevant technical topics, as well as shorter breakout sessions in specific areas. We are also planning special evening activities to facilitate networking and relationship building within the industry.

An agenda for this event should be available in early February with registration opening shortly thereafter. For more information, contact us at education@energysec.org

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 in the near future.

RSA ISAO Meeting

A chance to connect with your peers

Are you going to the year's RSA Conference? EnergySec staff will be in attendance and would love to connect with anyone in our community that will be there. Drop us a note at isao@energysec.org.

EnergySec has been provided meeting space by the Conference for the purpose of connecting with our community. We will have 45 minutes on Wednesday afternoon (location TBD) to meet and interact with others from our industry. EnergySec will have five staff members at the event and we invite anyone interested in meeting our staff and learning more about what we do to join us there. Watch for more information in the next couple of weeks as details are finalized.

The Vermont Non-Attack

An Editorial on Trust

[The following is adapted from comments originally published in EnergySec's Weekly Update, one of our publications provided to organizational members.]

In late December, the Washington Post published a story alleging that a small utility in Vermont had been targeted by Russian hackers. They soon retracted the story as more information became available regarding the underlying circumstances, little more than a routine hit on broadly applicable indicators. The news spread rapidly and received a great deal of attention, but the most important points were overlooked by most.

The real story here has been nearly universally missed by the news coverage, but demands attention. A small utility, heeding years of urging from industry and government leaders, filed a report to notify authorities of potentially malicious activity on their system. That was good. Very good. Less than 24 hours later, that information had been leaked to the press and published by the Washington Post. That was bad. Very bad.

Making matters worse, the leaked information was inaccurate, reflected faulty analysis (or no analysis at all), and was quite likely leaked for political purposes to support the ongoing assertions of Russian hacking. And, as noted in the highlights above, the underlying government information that formed the basis of the utility report, was of poor quality. This has been confirmed in private conversations I've had with various individuals in analysis roles at utilities and security providers.

NERC via the E-ISAC, the major trade organizations, government officials, and even we here at EnergySec have been banging the drums of information sharing for years. That effort is starting to pay off and sharing has been increasing as attention is focused on security issues at utilities large and small. But, sharing relationships are built on trust and must be mutually beneficial. This fiasco undermines both those requirements.

It appears that someone, likely a U.S. government official, violated the trust placed in them by the utility in reporting this information. Worse yet, the breach of trust appears to have occurred for reasons other than the common good. There is no benefit to industry or security in general in leaking such a report, especially with so little confirmed information at the time.

It is encouraging to hear Burlington Electric and others in industry remain publicly committed to sharing information and working together on cybersecurity, even in the face of this leak. However, I would be shocked if, behind closed doors, many utilities are not seriously reconsidering their level of transparency on cybersecurity issues. If trust is not maintained, future requests for information sharing may be met with a reception that is chillier than the waters of Lake Champlain in January. Let's hope that doesn't happen.

LITTLE BOBBY
by Robert M. Lee and Jeff Haas
SO WHAT ARE YOU STUDYING?
BUDGETING AND POLICY.
WHY NOT TECH SKILLS?!
I WANT TO BE A CYBERSECURITY EXECUTIVE IN GOVERNMENT OR BUSINESS ONE DAY...
...AND THAT IS WHAT'S ON THEIR RESUMES.
TRY TO DO BETTER.
KAPERSKI'S PIZZA
HAAS