Volume 2, Issue 4

INFRAGARD – NORTH CAROLINA

ncinfragard.org

Will it be "Lights Out" for the Energy Industry? Don't Panic. Plan Instead.

Theresa Payton, Charlotte Chapter VP

The Energy Industry Has Made Great Strides In Cybersecurity, However Cybercriminals Are Upping Their Game...Are You?

The last 18 months of headlines are not just a rough patch for the energy industry regarding cybercrime. They are a sign of escalating threats and new tactics deployed by cyber criminals. Need proof? “Cyber security“ as a forced rank priority moved last year to the top 3 risk factors faced by businesses on the Lloyds of London Risk Index. If cyber security were a world cup soccer team, that’s the equivalent of Brazil’s climb to fourth place headed into the 2014 World Cup which put them at their at their highest spot on the global ladder since July 2011.

And it’s not just the large energy companies that show up on the radar of cyber criminals. Every component of the energy supply chain is a target. From back office billing operations to in-the-field drilling platforms, smart grid connections, local substations, and county owned energy companies. “Nearly all categories of ‘sensitive US economic information’ are likely to be targeted…. energy and natural resources are a particular focus. These include secret operations and project information of US and other international oil and petrochemical companies. With commodity prices surging until recently, nations are anxious to find out all they can about what resources are available – and the latest technologies for extracting them.”1

The first question energy executives typically ask me, "How much security is enough security?".

The answer is a complex one and should be individualized to your organization's risk tolerance. Consumers and business professionals alike should focus on the fact that internet security will always be changing. Every new technology that we adopt becomes tomorrow’s attack surface for cyber criminals. Combating internet threats requires a comprehensive approach, some of these components include understanding your data architecture, truly knowing your vendors and challenging them to protect you better, sharing information within your peer group about cybercrime, developing relationships with law enforcement, implementing tools, updating processes to protect your digital assets and educating employees, contractors, and suppliers on what you require them to do in order to safeguard your organization.

Symantec, the security software company, indicated that their research shows that one cyber criminal group was specifically targeting firms that generate and transmit electricity as well as the petroleum pipeline operators. Their point of entry? Hacking into the control systems tied to equipment at the energy company. The Department of Homeland Security also warned back in May about increased targeting of the industrial control systems that are accessed over the Internet by cyber criminals. There was also an alert from the security company, CrowdStrike, about how “Energetic Bear” was targeting the intellectual property of energy companies in the US and abroad and looking for information to disrupt the power supply. The FBI also outed the hacker known as “UglyGorilla” this year. This hacker and others wanted to access US utility components that would allow them to damage pipelines. A U.S. grand jury indicted the ring of hackers in May but there are more like them that want access to your company.

Based on my time in the banking industry, the White House, and serving our clients, I have some ideas on how to change the conversation, save you time and money, all while improving your security posture. We have to change the security conversation.

Continued…

Inside This Issue

Lights Out for the Energy Sector?	1
Upcoming Events	2
Cybercamp Success	3
RED DART & ISI	4

Energy Industry Continued…

Instead of a pure tool focus, the emerging best practice for improving your threat posture is a focus on 4 rules:

1. golden rule: security & privacy first;
2. security=revenue;
3. WD40 your technology supply chain; and
4. you will be breached eventually, rapid response and recovery is key

Would You Accept A Bag of Balloons & Duct Tape As an "Air Bag" for Your Car? We can point to plenty of examples where security was built after the system was designed. When you do that, it feels as if a car sales person handed you a bag of balloons and duct tape and said, "This is your car's air bag, be safe!". Security and customer privacy must be your golden rule before you build one framework.

The critical infrastructure systems used in electrical power distribution, oil and gas pipelines, and the rest of the energy supply chain are vulnerable as their aging legacy architecture becomes easier and easier to compromise. A prediction for 2015 - a new wave of strikes on energy companies that have not migrated their critical systems away from the Windows XP operating system. Support ended April 2014 and those that remain on Windows XP are in peril.

Security can be a revenue generator. How does that happen? By forming a security practice in your company with a framework to formulate ideas and foster innovation. Some of the best and brightest security teams do not realize they have rusty leaks in their supply chain.

WD40, or the way to prevent and remove rust, requires an upfit and update of your vendor management program. This includes asking all vendors and suppliers the tough questions about how they protect your information from attack and what their incident response plan looks like. Review your control systems to make sure there are no direction connections to your business networks. Often times, a connection is made that seems harmless such as connecting usage from the control system to the back office for generating customers' bills. That connection could be the highway that cyber criminals use to target your control systems from your back office. All energy companies should practice a digital disaster at least two times a year. Name your worst digital nightmare and create a scenario based exercise to test out your rapid response and recovery plan. Make it realistic, time yourself, and grade your performance during the exercise. Be brutally honest with yourself about what is missing in your rapid response plan and work on improving your grade.

Upcoming Events

Charlotte Evening Meeting
Date/Time: Wednesday, October 14 from 6-8 pm
Location: Dilworth Grille,
Charlotte, NC.
Register at www.ncinfragard.org

Eastern Carolina Chapter Meeting
Date/Time: Wednesday, October 22nd from 1-4 pm
Location: Cisco, #5, 1025 Kit Creek Rd,
Morrisville, NC.
Register at www.ncinfragard.org

Charlotte Chapter Meeting
Date/Time: Wednesday, November 19th from 1-4pm
Location: Microsoft, 8050 Microsoft Way,
Charlotte, NC.
Register at www.ncinfragard.org

Eastern Carolina Chapter Meeting
Date/Time: Wednesday, December 10th from 1-4 pm
Location: Cisco, #5, 1025 Kit Creek Rd,
Morrisville, NC.
Register at www.ncinfragard.org

SA James Granozio
InfraGard Coordinator
7915 Microsoft Way
Charlotte, NC 28273
704-672-6351
james.granozio@ic.fbi.gov

InfraGard Helpdesk/Tech Support
(877)861-6298
infragardteam@leo.gov

Cyber Camp Success

Our **Charlotte InfraGard** planned, developed and conducted our **first annual CyberCamp** for high school students in STEM//gifted-talented programs from the surrounding Charlotte area. We had fourteen, 9th-12th grade students for a week long action packed, challenging program. Microsoft provided the training facility and cafeteria, Dell provided laptops, Time-Warner Cable provided exercises & instructors, 30+ InfraGard member volunteers provided their time as counselors. The agenda covered Chinese puzzles, locking mechanisms, computer exercises around attacking & defending systems, investigative tools, techniques and forensics provided by our local FBI office covering systems and mobile devices, risks and safeguards to personal computing & online safety. They toured the FBI office and visited the gun vault with a presentation from the firearms/SWAT instructor including SWAT MRAPs & equipment. They heard about FBI internships. They learned about gaming fraud and misuse from Xbox officials. They had presentations on human trafficking, and various employment opportunities in the public and private sectors. They played various games to encourage out-of-the-box thinking. Winning teams were provided trophies and all received various gifts.

I would personally like to **THANK** all of those who contributed your valuable time and equipment to make this incredible program possible!! A special **THANKS goes out to SAC John Strong and our local FBI Office**, who provided many FBI personnel, instructors, equipment, software and their facility for a special tour that was a real highlight for the kids.

I would also like to THANK corporate & educational contributors; Microsoft, Time-Warner Cable, Dell, Paraben, Lance, SPX, SafeNet, FishNet, ACE, South Piedmont & Rowan-Cabarrus Community Colleges, Wake Forest Univ. & the National Science Foundation.

I want to highlight some individuals with whom we could not have done without over the last sixteen months of weekly effort; SA Jim Granozio (our FBI Coordinator), Cindy Green-Ortiz (our Camp Director), Jim Payne (our Microsoft host) & Oscar Gonzales (our educational facilities, funding, spearhead). From the bottom of my heart THANK YOU ALL!

We are currently working to maintain monthly contact with our CyberCamp graduates through starting an **IG CyberCamp Club**. We have already started planning for next summer's camp which we hope to expand to a 3 day 8th & 9th grade program and a weeklong program for raising 10th-12th graders.

To provide these programs we will need sponsorship $$$$ and volunteers, so let's get started and show the country how Charlottes leads in growing the next generation of Infrastructure Protection Leaders!! I presented our program to InfraGard National and over a dozen chapters are interested in starting local CyberCamps.

Gary Gardner – Charlotte Chapter President

RED DART & ISI

September was in a word “exciting.”
Most notable were the two FBI sponsored training seminars I attended. First was the RED DART security summit held in Durham North Carolina and the second was an Information Sharing Initiative (ISI) held at the FBI facility in Atlanta. These seminars are generally available to all InfraGard members so please do attend as your schedules allow.

The RED DART security summit’s primary focus here was defining counterintelligence (CI) and why it was important. I personally walked away with a better understanding the CI’s value proposition. High level, my take was primarily to protect corporate intellectual property (IP) by properly classifying assets and then limiting access to those assets. That despite multiple layers of protection, insiders are proven again and again the most effective penetration tool. Therefore training from RED DART covered topics like monitoring access to IP, identifying, documenting and reporting suspicious activity by insiders.

Second only to the awesome speakers, the handout material provided to construct a successful CI management and support program was superb. Speakers during this summit included Mr. John Strong, Special Agent in charge of the Charlotte division. Mr. Jonathan Oaks, Special Agent in charge of the Carolina field office for Naval Criminal Investigative services. Thompson Reuters Chief of Innovation, and many others.

The second training seminar was the ISI two-day event in Atlanta. Here the FBI and other intelligence agencies shared their unique look at information sharing and cyber needs with the private sectors. Specifically core objectives as it relates to identification, handling and protection of sharing sensitive information. With the context all along focused on our nation’s critical key infrastructure and key resources (CI/KR).

Throughout the two day agenda following each specific objective I particularly enjoyed that we were divided into small groups. Here we were then tasked with answering difficult questions on that objective (e.g. challenges surrounding private sector information sharing). Following each breakout session once reassembled the Deputy Directory and faculty member of the Naval Postgraduate School amongst others vetted our question responses. From topics like how collected information is secured, managed, shared within and between the organizations to obtaining information from the intelligence community no topic seemed uncovered.

Educator representation here was extensive. From the office of the Director of National Intelligence the Director for Private Sector Partnerships started by discussing information sharing and possible management models with the private sectors. Other speakers included Mark Ray, Special Agent who discussed topics like cyber information needs, polices, procedures and structure. And John Cronier, Special Agent discussed a topic that captivated us all, Weapons of Mass Destruction (WMD).

If any of you are interested in seeing the material provided during these training seminars please contact me.

Mike Hillier, Charlotte Sector Chief, Banking & Finance