ASIS INTERNATIONAL
Utilities Security Council
ASIS COUNCILS

Utilities Security Council
“The Current”
April 2016

Chairman’s Corner

In This Edition

Greetings Utilities Security Council Professionals.

Last month we discussed the support that a fellow USC peer received after their company experienced damage (sabotage) to critical infrastructure in a foreign country. In this case it was several transmission towers that were attacked by local terrorists. After reaching out to the USC members, they received numerous suggestions on protecting these types of remote critical assets within the environment that they existed.

Well, within the last two (2) weeks, we had a similar situation right here in the U.S., although it resulted in no damage being done. An individual in this case attached incendiary devices to transmission towers in Massachusetts. Federal and local law enforcement responded, as did a bomb squad and a military unit. It was also just announced that an arrest has been made.

From this incident though, there were several positive actions that occurred that I would like to highlight. As we all know, trying to contain the spread of information across social media is near to impossible, and this was no exception. The word spread across the industry, with various versions. I heard everything from *"towers were destroyed"*, to *"explosive devices were discovered"*. Of course those reports were incorrect.

Chairman’s Corner, *continued*

The first positive action that occurred was that after the numerous federal agencies, investigated this incident, they disseminated the facts about this situation at an unprecedented speed. Through official intelligence communications channels these agencies updated security professionals and asset owners across the industry, which allowed us to accurately communicate with our organizations as needed. This single accelerated process assisted asset owners in bringing calm to the situation.

Secondly, it brought confidence to the overall security and intelligence processes, because through our established relationships, liaison roles, and/or official security intelligence sources, we were made aware of the facts and circumstances in a timely manner. We were then able to communicate that information as a means of industry situational awareness.

Lastly, we received this intelligence information from multiple official sources. We are all involved with task forces, intelligence and counterintelligence organizations, and industry organizations, which it was rewarding to see them all operate so effectively in distributing this information. What was even more rewarding was the personal contacts certain agency liaisons made to insure that their asset owner contacts were provided the most updated information.

I simply feel that we should give credit where credit is due, and for this particular incident, the communications process worked very well.

Utilities Security Council

Chairman

Anthony Hurley, PCI

1st Vice-Chairman

Nick Santillo, CPP, PSP, PCI

2nd Vice-Chairman

Mark Crosby, CPP, CISSP

Secretary

Scott Stephens, CPP

Council Vice President

Darren Nielsen, M. Ad, CPP, PCI, PSP, CISSP, CISA, CHHP, CBRM, CBRA

COMMITTEES/Chairperson:

Membership

Michael Ainslie, CPP

Women in Security

Sarah Bynum, CPP, CISSP

Guidelines & Standards

Matthew Dimmick, PSP

Annual Seminar

Mike Nagina, CPP

Certification Liaison

Paul Stanley, CPP

Newsletter Editor

Jeffrey S Leonard, CPP, PSP

Young Professionals

Mike Smith, CPP

Program Workshop

Doug Powell, CPP, PSP

Mentoring Project

Luis Morales, CPP

CIWG (Critical Infrastructure Working Group)

Jeff Campbell, CPP

Latin America

Jose Correa, CPP

Subject Matter Experts

Brian Harrell, CPP

White Papers

Ben Jakubovic, CPP

Chairman’s Corner, *continued*

On another topic, last month I mentioned a local university that was working with me and another ASIS International member (CPP) from another sector to develop specialized emergency management, preparedness and response courses. Last week that university invited me to speak as a guest lecturer, which I accepted. I spent several hours with thirteen (13) Master’s degree students discussing security, terrorism, incident preparedness and response. I also discussed ASIS International, and the benefit of getting involved with the organization as they pursued their professional careers. Again, I made a commitment to do a better job of 'getting the word out' about ASIS and our council in particular.

Lastly, I wanted to close by announcing that after a lot of studying, last Saturday I sat for the CPP exam. The preliminary test center results were that I successfully passed the CPP exam. I am committed to the ASIS International organization, and to this council. Just read the last several USC Newsletters and you will see our council peers continue to develop their credentials, even though they are well established within the industry and within their respective organizations. For this reason I decided to do the same. I sincerely thank everyone that offered study advice and words of encouragement.

Stay vigilant, remain aware of your surroundings, and most importantly, be safe.

Best regards,

Anthony Hurley, PCI, MEP (CPP Pending),
Chairperson, ASIS Utility Security Council (USC)
Utility Professional

Article

<u>Franklin v Tyson – the case for human performance during major events</u>

The 18th century statesman Benjamin Franklin exhorted that '*An ounce of prevention is worth a pound of cure'*. And recent DHS and NERC advisories[1] issued in the aftermath of the Ukraine Cyber Attacks of 2015 endorse that wisdom, providing comprehensive instructions and preventive technical measures to harden US utilities cyber systems against attacks.

The Ukraine report <u>is</u> sobering reading; multiple attack vectors disrupted power supply, obstructed recovery methods and bombarded call centers with DDOS attacks which impeded providers' ability to communicate with customers. But while prevention efforts are crucial they should not be the sole focus of our efforts. The attackers' tactics showed diverse methods clearly intended to overwhelm the targets, to disrupt not only IT and Command and Control systems, but also to frustrate individual response efforts to restore operations and to manage the emergency.

The dynamic and complex nature of the Ukraine attacks remind us of the need for human response capabilities and for organizational resilience to ensure that a crisis event doesn't metastasize into a disaster.

[1]

DHS IR-ALERT-H-16-043-01P UKRAINIAN POWER OUTAGE EVENT,
NERC advisory 'Mitigating Adversarial Manipulation of Industrial Control Systems as Evidenced By Recent International Events'

Of course not all incidents are a crisis. BS 11200[2] suggests that a crisis will have the following characteristics:

Unforeseen, poorly managed incidents or foreseen but the impact underestimated
Sudden onset or slow burner
High sense of urgency with greater effort required to achieve resolution
Can be complex & dynamic, not easy to understand & can present ambiguity & uncertainty
Can attract significant public & Media attention threatening reputation
Require flexibility, creative thinking & organisational resilience

The CSO must be able to differentiate between incident handling, which requires specific plans and responses, and crisis management, which demands a *strategic* response to minimize and manage the impact in many elements for the business, including image, reputation, long term operability, legislative and regulatory issues, communications and the media, stakeholder management and finance.

[2] BS11200 – British Standard on emergency and crisis management

The importance of setting up a Crisis Team

More recently, the famous 20th century philosopher Mike Tyson remarked ‘*Everyone has a plan until they’re hit’.* He used this description to explain the difficulty of predicting behavior and tactics in the boxing ring once you have taken a punch to the face.

The analogy is useful in considering company behavior during a sustained and complex cyber-attack, a mass casualty event or a weather disaster. Setting up and training a crisis team is not something that can be easily accomplished when you are on the ropes, reeling from the punches.

Consider the issues of availability, training and readiness. The company’s Crisis Team is normally headed by the chief executive, supported by coordination and legal experts, documentation and logistics resources. Depending upon the scenario typical membership may also include comprise senior IT, HR, Security, Facilities and Product line and Supply chain experts. These individuals and deputies must be identified ahead of time.

In establishing a Crisis Team for the company the CSO needs to assess individual capabilities and traits for the best team results. People will respond in different way to stress; to unstructured, dynamic situations, to missing or inconsistent information. Not everyone has the right traits to be part of the team.

Prior training and exposure to (simulated) dynamic complex scenarios is essential. Crisis team members will find ambiguity and conflicting information and must consider their decisions across an array of political, environment, societal and technical, economic and legal (PESTEL) factors. It will be helpful to consider human behavior elements affecting decision making and group behavior. Measuring the teams effectiveness needs to be done before it is tested in a live situation.

But on the plus side, crisis management contributes to organizational resilience in a generic way, while most incident handling methodologies only mitigate against specific attack scenarios. A meaningful description of capabilities can be an important decision point for customers. And as the CSO will act as the principle coordinator of the team it also provides an opportunity to forge valuable relationships with key decision makers and there's no downside to that.

Technical prevention measures and understanding attack methodologies will always be an important part of a business's preventive and detective posture. But even as we address hardware and software, let us not ignore the contribution of human performance to our readiness.

Sarah Bynum

Director of Security
Siemens Energy Inc. Orlando

Industry News

Training Event Focuses on Utility Cyberattack

The Indiana Department of Homeland Security led a tabletop exercise focusing on a cyberattack causing utility disruptions. Public and private cross-industry partners participated in the “Crit-Ex” exercise. Representatives from the energy and water industries, private sector information technology, and local, state, and federal government, including the Indiana Intelligence Fusion Center, were among those who took part.

The article is available at https://clicktime.cloud.postoffice.net/clicktime.php?X=XID927ucRNtJ0110Xd3&U=http%3A%2F%2Fwww.batesvilleheraldtribune.com%2Fnews%2Flocal_news%2Ftraining-event-focuses-on-utility-cyberattack%2Farticle_4d8cc0e7-0e64-5d7b-8d12-b1682bdfbc54.html&T=PINK&HV=X,U,T,S&H=103dadb84d555f234b038ef2e864e0762e93c143&S=Y.

Cyber resources are available at https://clicktime.cloud.postoffice.net/clicktime.php?X=XID927ucRNtJ0110Xd3&U=www.iacpcybercenter.org&T=PINK&HV=X,U,T,S&H=41f727ce192a44031422aa8d4067f5b8126295f8&S=Y.

Commanders urge Pentagon to counter growing threat of cyber attacks on industrial controllers

By Bill Gertz

Two American military commanders are sounding the alarm on the growing threat to U.S. national security posed by cyber attacks on critical industrial control systems.

Northern Command chief Adm. William Gortney and Pacific Command's Adm. Harry Harris urged Defense Secretary Ash Carter to step up efforts to deal with the danger.

"We respectfully request your assistance in providing focus and visibility on an emerging threat that we believe will have serious consequences on our ability to execute assigned missions if not addressed – cyber security of [Defense Department] critical infrastructure industrial control systems," the admirals warned in a Feb. 11 letter.

The commanders, who both are charged with defending U.S. territory, said the Department of Homeland Security monitored a seven-fold increase in cyber attacks on critical infrastructure between 2010 and 2015, including digital strikes against platform information technology, industrial control systems, and supervisory control and data acquisition systems.

Platform information technology is a security term for essential computer software and hardware that must be protected for national security reasons, including industrial control systems and critical infrastructure control networks, such as smart grid technology for power grids.

The software is used to control the electric power grid as well as networks used to control water, fuel and other critical infrastructure controllers.

“Many nefarious cyber payloads—Shamoon, Shodan, Havex and BlackEnrgy – and emerging ones have the potential to debilitate our installations’ critical infrastructure,” the admirals warned.

The four types of malware identified by the commanders are sophisticated technologies used by foreign adversaries that could attack, disable and destroy critical U.S. infrastructures.

BlackEnrgy has been linked by security researchers to Russian government cyber attacks, including recent cyber attacks aimed at Ukraine’s electrical power networks.

Shamoon is a sophisticated malware that has been used against oil and gas infrastructure, including the cyber attack on Saudi Aramco that damaged 30,000 computers. That 2012 attack was linked to Iranian hackers.

Shodan is a search engine gathers masses of data from the Internet, including controllers used for critical industrial systems. The software uses artificial intelligence to search out all Internet-linked devices. It has reached out to 100 million devices since it was first introduced in the 2009. Foreign adversaries are believed to be using Shodan for reconnaissance operations against U.S. infrastructure, in preparation for future cyber attacks.

Havex is a malware configured as a Remote Access Trojan that has been detected by security researchers targeting industrial control networks.

Havex has been used to scan local area networks for devices to Open Platform Communications, a standard used to send commands between SCADA applications and process control hardware.

As military commanders with homeland defense responsibilities concerned about the growth of the cyber-linked world, Harris and Gortney called on Carter to do more against cyber threats to critical infrastructure. Copies of the letter, first disclosed by Federal Computer Week, were also sent to senior military and security officials.

The letter is an unusual appeal from the military about one of the most important national security issues facing the country. It reflects the growing concern within the military about the danger of cyber attacks that could cripple the country in both peace and wartime – often without fully knowing the origin of the attack.

The main threat to infrastructure comes from Russia and China and both countries' intelligence services have been detected penetrating U.S. industrial control networks in reconnaissance operations – what the military refers to as preparation of the battle space for future attacks.

Currently the 16 critical U.S. infrastructures are vulnerable to cyber attack from China and Russia. But the most critical infrastructure of all is the electrical grid, the backbone upon which all other interconnected networks and systems rely.

The problem is not new. Reports from 2009 revealed that both the Chinese and Russian have penetrated critical infrastructure. “The Chinese have attempted to map our infrastructure, such as the electrical grid. So have the Russians,” a senior intelligence official told the Wall Street Journal that year.

The cyber attacks on grid networks involve the planting of clandestine “sleeper agent” software that remains dormant and undetectable in peacetime. In wartime, the software is triggered remotely, normally in the early stages of a conflict, to bring down systems, in the case of electric grid, to turn out the lights – and everything else that relies on electricity and lacks backup power sources.

Military planners in recent years have begun war-gaming future conflicts involving cyber attacks on critical infrastructure. The results are said to have been alarming. Targeted sophisticated cyber strikes to shut down power and other infrastructures can be carried out with devastating impact, and in coordinated stages and campaigns designed to force the quick defeat of the United States in a war.

Solutions are being worked on, such as developing new or redundant electrical power sources, stockpiling electrical transformers that are difficult to replace along with other measures. Pentagon researchers recently testified to Congress that exotic ways to generate electricity are being studied, such as creating microscopic organisms that consume metal and give off electricity

The massive efforts to gather intelligence on the U.S. critical infrastructures by both China and Russia has also been underway for more than a decade and little has been done to counter or dissuade the spying.

For example, China's hacking of the U.S. Transportation Command discovered several years ago has focused largely on how the Chinese might use the information to disrupt the critical logistics supply chain that is the strategic power of U.S. global military operations. Analysts say the intelligence from Transcom also is useful for the People's Liberation Army to prepare cyber pre-conflict cyber attacks on electrical grids in areas used in Transcom's operations, further compounding the difficulty of supplying military forces.

Unsaid by Gortney and Harris in the letter is the danger of cyber attacks on the infrastructure used by military bases, weapons systems and command and control.

On Russian SCADA operations, Director of National Intelligence James Clapper disclosed in September that Russia was working to remotely access industrial control systems used in U.S. critical infrastructures.

"Unknown Russian actors successfully compromised the product supply chains of at least three [industrial control system] vendors so that customers downloaded malicious software

designed to facilitate exploitation directly from the vendors' websites along with legitimate software update," Clapper stated in congressional testimony.

The malicious software used by the Russians in critical infrastructure attacks was identified as BlackEngry, the same malware detected in recent efforts by Moscow to turn out the power in Ukraine.

Critical infrastructure cyber attacks are among the most significant dangers facing the nation as the threats from both China and Russia continue to advance. As Gortney and Harris note, more work needs to be done to prepare for and counter the threat from cyber attacks to infrastructure, including developing cyber deterrence with demonstrations of U.S. cyber warfare power. So far, President Obama and his administration have shown no inclination to use American cyber power to develop such deterrence.

— Feb. 28, 2016

Belgium Fears Nuclear Plants Are Vulnerable

From "Belgium Fears Nuclear Plants Are Vulnerable"

New York Times (03/26/16) Rubin, Alissa; Schreuer, Milan

In the wake of the March 22 bombings in Belgium, authorities are focusing on the vulnerability of the nation's nuclear installations. Concerns have grown that the Islamic State is seeking to attack nuclear installations or obtain nuclear or radioactive material. This is especially worrying in a country with a history of security lapses at its nuclear facilities, a weak intelligence apparatus, and a deeply rooted terrorist network. On March 25, the authorities stripped security badges from several workers at one of two plants where all nonessential employees had been sent home after the attacks at the Brussels airport and one of the city's busiest subway stations three days earlier. Video footage of a top official at another Belgian nuclear facility was discovered last year in the apartment of a suspected militant linked to the extremists involved in the Paris attacks in November. The fears at the nuclear power plants are of "an accident in which someone explodes a bomb inside the plant," says Sébastien Berg, the

spokesman for Belgium’s federal agency for nuclear control. "The other danger is that they fly something into the plant from outside." That could stop the cooling process of the used fuel, and in turn shut down the plant. The revelation of the video surveillance footage was the first evidence that the Islamic State has a focused interest in nuclear material. But Belgium’s nuclear facilities have long had a worrying track record of breaches, prompting warnings from Washington and other foreign capitals.

Share | Web Link | Return to Headlines

Google Search Technique Aided N.Y. Dam Hacker in Iran
From "Google Search Technique Aided N.Y. Dam Hacker in Iran"
Wall Street Journal (03/28/16) Matthews, Christopher M.

Hamid Firooz, the Iranian charged with hacking the computer system that controlled a New York dam, used a readily available Google search process to identify the vulnerable system, according to people familiar with the federal investigation. Anyone with a computer and Internet access can perform the process, known as "Google dorking" with a few special techniques. Federal authorities said it is increasingly used by hackers to identify computer vulnerabilities throughout the United States. People briefed on the investigation said Firoozi stumbled onto the Bowman Avenue Dam in Rye Brook, N.Y., in 2013 by using the technique to identify an unprotected computer that controlled the dam’s sluice gates and other functions. Once he identified the dam, he allegedly hacked his way in using other methods. "He was just trolling around, and Google-dorked his way onto the dam," one person familiar with the investigation said. Cybersecurity experts said the search technique is neither illegal nor malicious.

Share | Web Link | Return to Headlines

Member Profile

Sarah Bynum, CPP, CISSP

Sarah Bynum CPP, CISSP is Sr. Director of Security at Siemens Energy Inc., headquartered in Orlando Florida. Siemens is a global equipment and services supplier to the power generation, distribution and transmission sector.

Bynum holds the M.Sc in Industrial Security and Risk Management from Leicester University in England. She joined Siemens 18 years ago after moving to the US following a 20 year career with Hampshire Constabulary as a Detective Sergeant and Inspector.

During her police career she was one of the first female detectives seconded to Lord John Stevens enquiry into collusion between Loyalist terrorists and Military personnel in Northern Ireland. At Siemens she was part of the early team assessing Iraq’s power infrastructure in 2003 following the end of combat operations.

Bynum is responsible for physical security, security of project locations and personnel traveling overseas, investigations and crisis management; while a growing area of interest is the assessment of suppliers for collaboration and information sharing in offshore locations. She is most proud of her opportunities to mentor other women in the security profession.

She is an enthusiastic watersports fan, enjoying sailing, diving and kayaking. Living in Central Florida allows her plenty of opportunity to enjoy the lakes and rivers which abound here.

ASIS INTERNATIONAL
Utilities Security Council

ASIS COUNCILS

Utilities Security Council

A Monthly Newsletter of the ASIS International Utilities Security Council (USC)

(Editor's Note: This newsletter is published for the use of USC members and other interested ASIS International security councils, working groups, leaders, members and staff. It is not an official publication of ASIS International. As such, the information and articles contained in this, and subsequent editions of "The Current", should be considered as unofficial and for member interest and use as appropriate)

ASIS INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, VA 22314-2818
USA
703-518-1447
Fax: 703-518-1517
Email: *councils@asisonline.org*