White Paper

Physical Protection of Critical Electric Infrastructure
–
A U.S. Perspective

© 2016

For Additional Information Please Contact:

Toll Free: 877-914-2780

sales@securicon.com

www.securicon.com

Note:

This White Paper is derived from the original article published by the Author in the Caspian Strategy Institute Blog on 28 January 2016.[1]

The Attack

The attack occurred on a large transmission substation just south of San Jose, California USA. It was a moonless night, around 48° F with a light breeze from the west. At 12:58 AM the adversaries began their attack.

First they surgically cut important telephone cables used for two-way communication for the substation. Then, the cable cutters waved a lit flashlight giving the shooters the go ahead to open fire.

At 1:31 AM the adversaries opened fire with rifles on the substation for about 19 minutes knocking out 17 large electric transformers used to transfer electricity into Silicon Valley. The gunmen appear to have aimed at the transformers' oil-filled cooling systems. The transformers leaked around 52,000 gallons of the cooling oil then ultimately overheated resulting in failure of the first transformer about 15 minutes after the shooting began and causing alarms at the utility control center.

The plans for this attack were so detailed and precise that the 100+ shell casings from the AK-47 rifle bullets were free of any fingerprints.

The attack described above occurred on Tuesday, 16 April 2013 at the Metcalf Transmission Substation operated by Pacific Gas & Electric[2] and probably the best summary of the attack is from an article in the ***Wall Street Journal*** dated 5 February 2014.[3]

The Beginning of New Regulations

Ever since the mid-2000's the United States Federal Energy Regulatory Commission (FERC)[4] has been directing the North American Electric Reliability Corporation (NERC)[5] to oversee most electric utilities in North America operating electric transmission to comply with a collection of Critical Infrastructure Protection (CIP)[6] standards focused on protecting the electric grid from cyber-attack. Until the event at Metcalf there has been minimal regulatory focus on physical protection of critical electrical infrastructure.

---

1 http://www.hazar.org/analizdetail/analysis/physical_protection_of_critical_electric_infrastructure_%E2%80%93_a_us_perspective_1466.aspx

2 www.pge.com

3 Smith, Rebecca. "Assault on California Power Station Raises Alarm on Potential for Terrorism." ***The Wall Street Journal***, 2014. http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778

4 www.ferc.gov

5 www.nerc.com

6 http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

However, with the Metcalf attack, the attitude by the US Government, California State Public Utilities Commission, electricity technology and lobbying organizations, and FERC substantially changed when it came to protecting substations and other critical electric infrastructure from more severe attacks beyond simple vandalism and metal theft.

At a California Public Utilities Commission meeting in 2014 to review the incident, the PG&E senior director of substations said the Metcalf attack was "a game changer."

"No doubt about it …this event caused us and the entire industry to take a new and closer look at our critical facilities and what we can do to protect them," he said.[7]

On 7 March 2014, FERC issued an order[8] directing NERC to *"…develop and file for approval proposed Reliability Standards that address threats and vulnerabilities to the physical security of critical facilities on the Bulk Power System. Such Reliability Standards will enhance (FERC's) ability to assure the public that critical facilities are reasonably protected against physical attacks."*

What was particularly unusual in this FERC order was the speed at which it was issued – within a year following the Metcalf event – and FERC's expectation that NERC submit the proposed Reliability Standards within 90 days of the date of the order.

In spite of some criticism of the speed needed to develop these new proposed Reliability Standards NERC issued CIP-014-1, Physical Security, on 5 May 2014 – well within the 90 days mandated by FERC.

On 20 November 2014, FERC issued its order[9] approving CIP-014-1 but with some comments ultimately requiring a revision to the standard. CIP-014-2 – Revision 2. The new and final Standard was issued by NERC and approved by FERC on 14 July 2015.

CIP-014-2 Physical Security[10]

The purpose of CIP-014-2 is:

> *To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.*

The Standard applies to transmission substations operating at greater than 500 kV[11] and selected substations operating between 200 kV and 499 kV based on identified criteria.

---

[7] Reilly, Steve, and Ryan Sabalow. "Bracing for a Big Power Grid Attack: 'One Is Too Many' - NBC News." Accessed January 27, 2016. http://www.nbcnews.com/news/us-news/bracing-big-power-grid-attack-one-too-many-n329336

[8] https://www.ferc.gov/CalendarFiles/20140307185442-RD14-6-000.pdf

[9] https://www.ferc.gov/whats-new/comm-meet/2014/112014/E-4.pdf

[10] http://www.nerc.com/pa/Stand/Prjct201404PhsclScrty/CIP-014-2_Physical_Security_2015Jan30_clean.pdf

The Standard includes six requirements summarized below:

Requirement 1:

Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its transmission stations and transmission substations (existing and planned to be in service within 24 months)

Requirement 2:

Each transmission owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The unaffiliated third party verification shall verify the transmission owner's risk assessment performed under Requirement R1, and which may include recommendations for the addition or deletion of a transmission station(s) or transmission substation(s).

Requirement 3:

Requires notification of appropriate control centers that manage/operate the selected transmission substations of the risk assessment results/analyses.

Requirement 4:

Each transmission owner that identified a substation or primary control center in Requirement 1, and verified same according to Requirement 2, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective assets identified in R1 and R2.

Requirement 5:

Each transmission owner that identified a transmission station, transmission substation, or primary control center in the above steps shall develop and implement a documented physical security plan(s) that covers their respective transmission station(s), transmission substation(s), and primary control center(s).

The physical security plans should address:

- Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted above.
- Law enforcement contact and coordination information.
- A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

[11] kV = Kilo Volt or 1,000 volts

- Provisions to evaluate evolving physical threats, and their corresponding security measures, to the transmission station(s), transmission substation(s), or primary control center(s).

Requirement 6:

Each transmission owner affected above shall have an "unaffiliated third party" review the evaluation performed in Requirement 4 and the security plan(s) developed under R5. The unaffiliated third party must be from the following:

- Entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either an ASIS Certified Protection Professional (CPP)[12] or Physical Security Professional (PSP)[13] certification; or,
- An entity or organization approved by NERC, or,
- A governmental agency with physical security experience, or
- An entity or organization with demonstrated law enforcement, government or military physical security expertise

Helpful CIP-014-2 Implementation Guides

The CIP Standard itself is unique in that it really is focused on physical protection of transmission assets and not on cyber issues. Because of this new perspective and difference from the other CIP Standards some very helpful guidance on implementing CIP-014 has been built by the North American Transmission Forum (NATF)[14] headquartered in Charlotte, North Carolina USA.

NATF has issued three very helpful guides on implementing CIP-014 requirements 1, 4 and 5. These guides may be useful for other national electric transmission entities looking to improve the physical security of their critical electric infrastructure.

- NATF CIP-014 R1, Guideline V1[15]
- NATF Practices Document – CIP-014 Requirement R4[16]
- NATF Practices Document – CIP-014 Requirement R5[17]

[12] https://www.asisonline.org/Certification/Board-Certifications/CPP/Pages/default.aspx
[13] https://www.asisonline.org/Certification/Board-Certifications/PSP/Pages/default.aspx
[14] www.natf.net
[15] http://www.natf.net/wp-content/uploads/NATF-CIP-014-1-R1-Guideline-V1-Open.pdf
[16] http://www.natf.net/wp-content/uploads/NATF-Practices-Document-NERC-Reliability-Standard-CIP-014-1-Requirement-R4.pdf
[17] http://www.natf.net/wp-content/uploads/NATF-Practices-Document-NERC-Reliability-Standard-CIP-014-1-Requirement-R5.pdf

The last two Practices Documents are especially helpful in that they include forms and data collection formats for physical security information collection and ultimate development of physical security protection plans for the critical transformers/substations.

State of California Weighs In on Physical Security for Critical Electric Infrastructure

The investor-owned electric utilities in the State of California are regulated by the California Public Utility Commission (CPUC)[18]. Because the Metcalf event occurred at one of the state-regulated utilities' facilities the CPUC began examining electric grid security at all levels including the distribution voltage level i.e., the lower voltages being sent to businesses and homes. The CPUC views its mandate to enforce physical security of all electric grid assets for their regulated utilities and they are developing rules beyond the FERC / NERC requirements of CIP-014-2.

The California State Senate issued Senate Bill 699[19] – which was approved by the Governor in September 2014. The bill would require the CPUC to consider adopting rules to address physical security risks to the distribution system of electrical corporations.

New Analysis from the Electric Power Research Institute (EPRI)

In April 2015 the Electric Power Research Institute (EPRI), headquartered in Palo Alto, California USA, issued a report entitled ***Assessing and Enhancing the Security of Transmission Assets from Intentional Physical Attack[20].*** The report is an excellent summary read for anyone on this subject and includes some interesting statistics on the number of attacks on transmission lines, towers/pylons, and substations derived from the US State Department.

About the Author

Ernie Hayden is a highly experienced and seasoned technical consultant, author, speaker, strategist and thought-leader with extensive experience in the industrial controls security, power utility industry, critical infrastructure protection/information security domain, cybercrime and cyberwarfare areas. His primary emphasis is on project and business development involving cyber and physical security of industrial controls, smart grid, energy supply, and oil/gas/electric systems and facilities with special expertise on industrial controls. Hayden holds certifications as a Global Industrial Cyber Security Professional (GICSP) with Gold amendment, Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and ASIS Physical Security Professional (PSP). Hayden is an Executive Consultant at Securicon, LLC, has held roles as Global Managing Principal – Critical Infrastructure/Industrial Controls Security at Verizon, held information security officer/manager positions at the Port of Seattle, Group Health Cooperative (Seattle), ALSTOM ESCA and Seattle City Light. Hayden is also a Non-resident Fellow at the Hazar Strategī Enstītüsü/Caspian Strategy Institute[21] headquarterd in Istanbul, Turkey. In 2012 Ernie was named a "Smart Grid Pioneer" by Smart Grid Today. Ernie is a frequent author of blogs, opinion

[18] http://www.cpuc.ca.gov/default.aspx
[19] http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140SB699
[20] http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002006354
[21] http://www.hazar.org/

pieces and white papers. He has been cited in the Financial Times, Boston Globe, Energy Biz Magazine, Information Security Magazine and Puget Sound Business Journal. Many of his articles have been posted to such forums as TechTarget/SearchSecurity, Energy Central, Public Utility Fortnightly "SPARK," and his own blog on Infrastructure Security[22].

About Securicon

Securicon provides expert consulting for application, system and network security, as well as physical security testing and assessments. Services include application security evaluations, source code analysis, secure application development training, penetration and vulnerability assessments, security architecture consulting, creation of security plans and policies, as well as compliance audits and consulting. In addition, we provide strategic consulting to customers such as the US Cyber Command in areas such as computer network defense, as well as supporting the FISMA and Risk Management Framework programs for many civilian agencies. Securicon supports both Federal, as well as critical infrastructure companies in the power & energy, oil & gas, pipeline, water and the financial services industry.

[22] http://infrastructuresecuritytoday.blogspot.com/