July 2012 / Issue 10

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

NERC Compliance Trends for 1st Half 2012

By all accounts, 2012 has been a busy year for NERC. The year-to-date (through July 31) total dollar fines issued by NERC is just over $2 million. NERC has reported an average of 257 violations per month and is currently processing 79 violations for the first half of the year in comparison with only one violation for the last half of 2011.

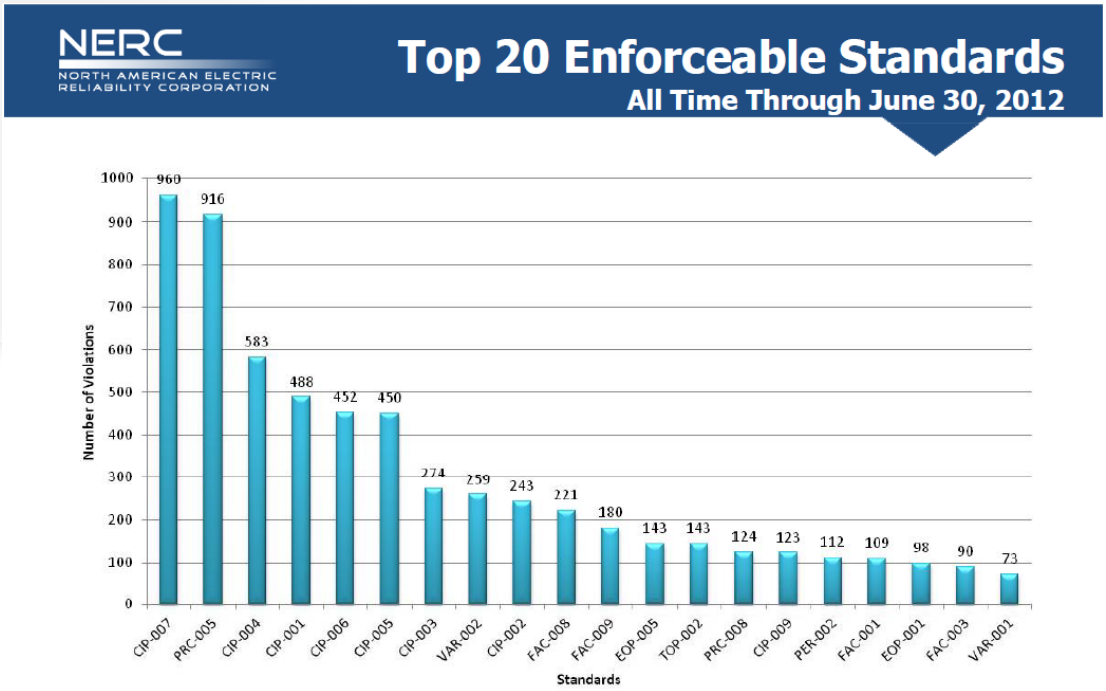
The impact of these activities are not lost on NERC-CIP. The following chart from NERC clearly shows that NERC-CIP compliance standards continue to make up the top enforceable standards for the agency. To understand how this impacts the Power Generation industry, read Tim Johnson's piece in the Consultant's Corner, "NERC-CIP Version 4: Are You Ready?"

July 2012
Cyber Attack Statistics
- Hackmageddon.com

Attack Motivations
- 69% Cyber Crime
- 23% Hacktivism
- 8% Cyber Espionage

Top 3 Attack Targets
- 38% Industry
- 10% Government
- 10% other Orgs

Top 5 Attack Techniques
- 53% Unknown
- 21% SQL
- 18% DDoS
- 8% Defacement
- 8% APT Attack



Industry News

Senators call for probe of electric grid cyber security

CNET.com, 7/18/2012

Two U.S. senators are calling for a federal investigation of the power grid's potential cyber security vulnerabilities after a CNET article last month raised security concerns. The request for a probe comes from Sens. Joseph Lieberman (I-CT), the chairman of the Senate Homeland Security Committee, and Susan Collins (R-ME), the panel's senior Republican, who warned that lapses "could undermine part of the security system protecting our grid." They sent a letter yesterday to the Federal Energy Regulatory Commission asking for an "expeditious comprehensive investigation into these allegations," which deal with digital signatures the industry uses for authentication.

Attacking SCADA and relative cost of entry

Darkreading.com, 7/19/2012

SCADA technologies have been increasingly targeted by shadowy adversaries: Does that mean impending doom? Earlier last month, a friend and industry colleague reported on a spear-phish that targeted an employee of well-known industrial control security firm Digital Bond. Like many targeted email spears, the message was generally well-written and demonstrated some domain-level experience in the arena of industrial control security. Attached to the email was a zip file containing an executable designed to masquerade as a PDF, that, when executed, downloaded a secondary payload, which, in turn, installed a RAT (remote access tool) onto the victim's PC.

DHS reports rise in water sector cyber attacks

AWWA.org, 7/7/2012

In a newly released report on incidents from 2009 through 2011, ICS-CERT documents that attack against water sector targets rose from 3 (of nine total) in 2009 to 81 (of 198 total) in 2011. The report further documents three onsite investigations of water sector targets. For one reported by a municipal water treatment plant, ICS-CERT concluded that "there was no targeted malicious activity" and that "overall cyber defense and incident response capabilities at this facility were low." Another found "an infection of the remote terminal server...[that] was non-targeted and consistent with crimeware, not a sophisticated threat." The third involved an apparent unauthorized login that turned out to be "an authorized user logging into the control system while on personal business in a foreign country for legitimate business purposes."

Anonymous targets oil giant Exxon

AWWA.org, 7/7/2012

Last week and continuing into the weekend, Anonymous targeted ExxonMobil and claimed to have compromised company data during Operation SaveTheArctic. The attack was in response to environmental concerns, and it isn't the first time Exxon has come under the gun with regards to the faceless hacking collective. "The energy companies that caused the Arctic to melt in the first place are looking to profit from the disappearing ice. They want to open up a new oil frontier to get at a potential 90 billion barrels of oil. That's a lot of money to them, but it's only three years' worth of oil to the world," Anonymous stated after the attacks.

Cyber incidents on the rise in US, but analysis shows flaws in basic security

Nextweb.com, 7/3/2012

A report from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) stating that cyber incidents jumped from 41 in 2010 to a stunning 198 in 2011, has sent industry watchers into a frenzy. What could cause such a massive rise? Putting those figures into perspective, only 9 incidents were reported in 2009, the year that ICS CERT was established. From 9 to 41 to 198 is quite the growth curve. In the last year, of the 198 incidents, 41% involved the water sector. When incidents that included multiple infrastructure genres are totaled, the water sector was part of more than half.

The current state of cyber (in) security in the electric industry

Community.controlglobal.com, 7/1/2012

NERC CIP Version 4 introduced the "bright line" concept, which sets a minimum threshold for size of power plants and substation voltage to be considered critical. Cyber is a common cause failure that can impact multiple facilities from multiple organizations—it is not a single node event. Examples like Slammer and Blaster demonstrate that point.

Cyber News

China lays out glorious eight-point infosec masterplan

TheRegister.co.uk, 7/19/2012

The Chinese government has released sweeping new information security guidelines designed to enable public and private bodies to protect themselves more effectively against new cyber threats. The State Council's long list of recommendations spans just about every conceivable aspect of information security, painting a picture of a nation under siege from attackers and increasingly vulnerable thanks to its reliance on the internet. It points to the need to better secure "energy, transport, finance and other fields of the national economy" as well as government departments. On the government side, the\ guidelines include more auditing, security reporting and monitoring, and a pledge to "reduce the number of internet connection points"—presumably to isolate highly classified data on specific machines.

Mobile phone users sorely mistaken about how much privacy they have

Arstechniacom, 7/12/2012

"We found that Americans overwhelmingly consider information stored on their mobile phones to be private—at least as private as information stored on their home computers," states the study, which used information collected by both landline and wireless phones. Fifty-nine percent of all respondents ages 18 to 65 and beyond said their phones were "at least as private" as their home computers, and 19 thought their phones were more private than their home computers.

Cyber chief warns of rising danger from cyber attacks

Security.blogs.cnn.com, 7/9/2012

In a rare public appearance Monday, the head of the country's Cyber Command warned that the nature of cyber attacks is changing and becoming more dangerous. Gen. Keith Alexander also talked about the economic toll that cyber intrusions are taking on American business, saying that for every intrusion detected by the FBI, there are 100 others that remain undetected. "The probability for crisis is mounting," said Alexander, who also heads the National Security Agency. He told an audience at the American Enterprise Institute in Washington that he was concerned about the changing nature of the threat from disruptive to destructive attacks and that the numbers of cyber attacks against business and critical infrastructure are on the rise.

Yahoo hacked, 450,000 passwords posted online

cnn.com, 7/12/2012

Hackers posted online what they say is login information for more than 450,000 Yahoo users. The hack, which of course was conducted anonymously, was meant to be a warning, according to the Web page where the documents were dumped. "We hope that the parties responsible for managing the security of this subdomain will take this as a wake-up call, and not as a threat."

Yahoo service SQL injection vulnerability leads to account exposure

Isc.sans.edu, 7/13/2012

An SQL injection vulnerability was leveraged to gain access to the Yahoo Voice service, which was used by attackers to acquire and then post login credentials for more than 453,000 user accounts that they said they retrieved in plaintext. Password analysis of the account list proved what we've all come to expect. "The top five passwords in the stolen batch were "123456," "password," "welcome," "ninja," and "abc123."

Consultant's Corner

NERC CIP Version 4: Are You Ready?

Version 4 of NERC CIP received final approval in April of this year, which primarily affects plants that are 1,500 MW or higher. Since the effective date for compliance is approximately two years after final approval, plants must have their NERC CIP program in place by April 2013 so that they are collecting evidence for audits that will start in April 2014. Although this may seem like a lot of time, it really is not given the amount of preparation required for a NERC-CIP audit.

CIP Version 4 has two items that DCS Managers must address:

1. **Critical Asset Identification**
   A Critical Asset is a group of generating units at a single plant location with an aggregate highest rated net real power capability of the preceding 12 months equal to or exceeding 1,500 MW in a single interconnection.

2. **Critical Cyber Asset Identification**
   Using the list of Critical Assets developed in the Critical Asset Identification above, the responsible entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that are in aggregate equal or exceed 1,500 MW.

DCS Managers must determine whether a site has Critical Cyber Assets. Without Critical Assets, each unit runs independent of any other unit at the site and no single cyber asset affects power production equal to or exceeding 1,500 MW; with Critical Assets, the DCS Manager may need our help complying with NERC CIP. See this link for more details: http://www.nerc.com/files/CIP-002-4.pdf.

Although many companies have compliance managers at their corporate office, we usually find that dealing with them involves their IT group, who wants to keep the bulk of the compliance work in-house. The DCS Manager usually prefers not to work with IT because they have little—if any—DCS experience. This, along with our NERC CIP expertise, gives Invensys an edge at these sites. In many cases, DCS Managers have a keen interest in NERC CIP because they can be held directly accountable for what was done or not done regarding compliance. If the site has no Critical Cyber Assets, it is the DCS Manager's responsibility to ensure no cyber assets are interconnected to equal or exceed 1,500 MW. The Invensys cyber security team can work the client to understand just what is a Critical Cyber Asset and carry out an assessment to get a better understanding of how many critical assets they have.

Questions to ask when setting up the initial meeting:

1. Have you determined whether your site is a critical asset under NERC CIP Version 4?
2. Do you have a plan and methodology to evaluate your critical cyber assets?
3. Are you willing to spend 30 minutes with our NERC CIP subject matter experts to discuss what we have learned and how we might help you?

This months contributor to Consultant's Corner is
Tim Johnson
Principal, Critical Infrastructure & Security Practice
Invensys
tim.johnson@invensys.com

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
July 2012 / Issue 10

Invensys Critical Infrastructure and Security Practice (CISP)

Invensys CISP has capability in establishing, implementing, and maintaining industry best practices to meet the demands for government regulations (NERC-CIP, NEI 08-09, CFATS), industry requirements, and company compliance requirements. Attributes of Invensys CISP include:

Hardware Independence

CISP can work with any type of control system or type of technology a customer prefers for the security environment.

Industry Knowledge

CISP has a number of resources that help them understand the demands of Control Networks and the requirements for continued uptime.

Regulation Knowledge

CISP has a number of subject matter experts who understand a whole host of regulatory requirements as well as actively participate in a number of industry and government groups.

Proven Methodology

CISP follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the life cycle approach are Assessment, Development, Implementation, and Management.

Technical Knowledge

The same CISP personnel who have regulatory knowledge are also well versed in the latest security policies, procedures, and technologies for intrusion detection and prevention, firewalls, DCS, and network architecture.

Join us on Blogger

invensys™

For additional information, please visit us at
http://iom.invensys.com/CyberSecurity

5601 Granite Pkwy. Suite 1000 Plano, TX 75024 ▪ P 214.295.6365 ▪ F 888.758.7675 ▪ **iom.invensys.com**