June 2013 / Issue 21

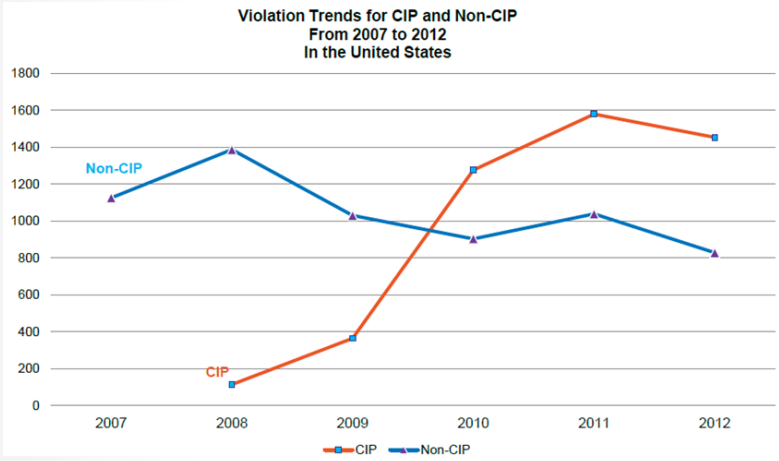
The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

NERC CIP Mid-Year Checkpoint

June marks the mid-point of the year, which is a good time to take a look at NERC CIP and how the numbers are adding up. NERC has been busy not only with NERC CIP v5, but also adjusting to the new landscape. As we mentioned back in the February 2013 Issue 17 newsletter, there has been shift in the NERC violation trends. Beginning in 3Q2010 CIP-only violations began increasing over non-CIP violations, illustrated in the chart below. Researchers predict this trend to continue as NERC is driven by the maturity of CIP, new versions of the standard, and the associated implementation plans.



Since June 2008, NERC violations have impacted 771 entities for a total of $22.5 million. How are new possible violations (NPV) discovered? The answer continues to be Self-Identification. In 1Q2013, external discovery (inspectors) was 22 percent and internal was a strong 78 percent.

Digging into the NERC details, you will see that more and more entities are in violation of CIP standards only, these being the CIP-002 through CIP-009 reliability standards.

The data below excludes entities that had both CIP and non-CIP NPVs since June 2008.

Total entities in violation of ONLY CIP standards:	63
Total CIP standards these entities were in violation of:	648
Total violation fines for ONLY CIP standards:	$5.1MM
That is an average fine per individual CIP NPV of:	$7,900 and growing

This year will continue to be a transition year for power companies and NERC, with a focus on CIP violations and a new CIP version on its way. Power companies will need to focus on cyber security compliance now more than ever.

June 2013
Cyber Attack Statistics
- Hackmageddon.com

Attack Motivations
- 46% Cyber Crime
- 36% Hacktivism
- 9% Cyber Espionage

Top 3 Attack Targets
- 24% Industry
- 21% Government
- 10% Organization

Top 5 Attack Techniques
- 32% SQL
- 21% Unknown
- 14% DDoS
- 12% Targeted Attack
- 9% Defacement

Industry News

NERC: Anxiety, regulatory uncertainty surround effective date of BES revisions

www.elp.com, 6/3/2013

On May 23, the North American Electric Reliability Corporation asked the Federal Energy Regulatory Commission for a one year extension to the effective date of its FERC-approved revisions to the definition of the bulk electric system (BES) "in the interest of regulatory certainty." NERC, which is charged with ensuring the reliability of the North American BES, said that though it is on schedule to implement the revised definitions of the BES by the current effective date of July 1, there would be a transitional period of time during which the existing definition would be in effect, which could result in unintended consequences that may ultimately thwart FERC's agenda to bolter reliability (FERC Docket Nos. RM12-6 and RM12-7). On Dec. 20, 2012, FERC approved NERC's revisions to the definition of the BES, finding that the revisions satisfied the directives of FERC Order 743. The commission on February 19 granted rehearing of the final rule. Order 743 required that the definition of the BES encompass all facilities necessary for an interconnected transmission system and remove regional discretion without review or oversight.

Critical Infrastructure Protection (CIP) market worth $105.95 billion by 2018

www.sacbee.com, 6/12/2013

The need for increasing the agility of a business process, along with cost control measures is playing a cardinal role in shaping the future of the Critical Infrastructure Protection market. Even though the adoption of these solutions is slow due to the high costs involved with deployment and compliance concerns, these solutions are expected to gain increasing market traction across all major verticals, owing to the growing demand for automation and secure connectivity. Markets and Markets further expects that the integration of security solutions within the existing organizational framework will further amplify the growth of businesses while ensuring the compliance and regulatory standards.

CFATS Fact Sheet update

chemical-facility-security-news.blogspot.com, 6/8/2013

The information below shows the data from the new CFATS Fact Sheet update as well as the similar numbers from the initial two updates.

June 2013

- Facilities currently covered by CFATS: 4331
- Removed, reduced, or modified COI holdings: 3000
- Facility Assistance Visits: 1253
- SSP Authorized: 469 (10.8%)
- SSP Approved: 125 (2.9%)

This new data shows continued improvement in the SSP approval process.

Control system security, 100,000 vulnerabilities

controlsystemsecurity.blogspot.com, 6/7/2013

The popular press cites an "alarming" statistic from time to time—the "dramatic" increase in cyber security vulnerabilities being reported in industrial control system components. 129 were reported in 2011, versus only 15 in 2010 and 14 in 2009. Those of us in the industry, of course, groan when we read nonsense like this. We know the truth to be rather more "dramatic." How bad is SCADA security, really? Let's do the math. Let's ignore PLCs, hardened network gear, hard-coded passwords, smaller software packages, smaller vendors, and everything else except buffer overflow vulnerabilities in major industrial software products. The back of the envelope reads:

50,000 * 2% * (10 * 3 * 5 *0.75) = 112,500 vulnerabilities

That's a conservative estimate. So there are at least 100,000 vulnerabilities waiting to be found out. This supports reports from security researchers who say they generally need to spend only a couple hours with each industrial software product they look at to come up with their first half-dozen vulnerabilities.

U.S. Energy Department creates cyber security council

www.infosecurity-magazine.com, 6/17/2013

The U.S. Department of Energy is tackling cyber security for its various branches, including the National Nuclear Security Administration (NNSA), with a new cyber security council tasked with formulating best practices in the security arena. Energy Secretary Ernest Moniz, who is three weeks into his tenure, told the House Energy and Commerce Committee that the council includes representation from the department's electricity office, the intelligence division, the office of the CIO, and the NNSA.

Cyber News

Industry-wide cyber security standards emerging through voluntary framework

www.elp.com, 6/12/2013

Reported cyber attacks on utility sector control systems increased more than 50 percent in 2012. The energy and water sectors represented most of those reported attacks. In addition to exploits that threatened supervisory control and data acquisition systems and other industrial controls, cyber attacks have affected operations and maintenance activities, billing and customer information databases, Web-based payment systems, PBX phone systems, and other Internet-facing networks and devices. This increasing risk to the electric sector and other critical infrastructure in recent years has pushed federal and state governments to investigate and in some cases advocate for utility cyber security measures. Despite statements from high-ranking officials such as the national intelligence director that cyber attacks are at the top of the nation's security threats, federal action has not kept pace with cyber threats confronting critical infrastructure networks.

Japan's New cyber security strategy—implications for the alliance?

www.forbes.com, 6/13/2013

On June 10, the Japanese government adopted the Cyber Security Strategy to replace the Information Security Strategy for Protecting the Nation, which was crafted in May 2010 and expires in March 2014. This is the first time for Tokyo to employ the word, "cyber security," in its strategy to deal with information security issues and cyber threats to its national interests. Japan is planning on creating an action plan based on this strategy by the end of June.

India prepares cyber security strategy

www.abc.net.au, 6/17/2013

India is preparing to roll out a new cyber-security system, amid reports it was among the top five countries compromised by U.S. surveillance. The National Cyber Coordination Centre's primary job is to carry out a real-time assessment of cyber security threats and provide actionable reports. According to data compiled by the Indian Computer Emergency Response Team, more than 1,000 government websites storing critical and sensitive data concerning national security have been hacked by cyber criminals in the last three years.

More malware is traveling on P2P networks these days

www.computerworld.com, 6/17/2013

Hackers have found a devious new way to disseminate malware: they're using peer-to-peer networks. Security firm Damballa reports that the number of malware samples that use P2P communications has increased fivefold during the past 12 months. Advanced threats like ZeroAccess, Zeus Version 3, and TDL 4 are playing the biggest roles in this development, said Stephen Newman, vice president of products at Damballa. Meanwhile, other malware families have adopted P2P as a command-and-control channel, he said.

Pentagon's cyber security plan calls for $23 billion through 2018

www.business-standard.com, 6/18/2013

A Pentagon cyber security budget outline calls for spending almost $23 billion through financial year 2018, as efforts are expanded on initiatives from protecting computer networks to developing offensive capabilities. The U.S. Defense Department already has proposed $4.65 billion for such programs in the financial year that begins October 1, an 18 percent increase from the $3.94 billion budgeted this year. The five-year "cyber expense" budget obtained by Bloomberg News calls for spending to remain elevated from past levels. Defense Secretary Chuck Hagel cited "the growing threat of cyber intrusions, some of which appear to be tied to the Chinese government and military." His predecessor, Leon Panetta, said last year that "a cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11."

Consultant's Corner

Leveraging a SIEM for Regulatory Audit Requirements

Security Incident and Event Management (SIEM) appliances are becoming a necessary tool for meeting industry regulatory audit compliance. Regulation requires industries to review and analyze audit logs for possible cyber incidents. The burden to review and analyze millions of audit events can be an insurmountable task. SIEMs lessen this burden by collecting audit logs from critical infrastructure assets, information technology infrastructure, and security appliances into a central appliance. To be an affective audit compliance tool, the SIEM must have adequately configured log sources, ample storage, and the ability to produce meaningful reports.

Log Sources

Log sources provide the necessary auditable events collected by the SIEM. The log sources must be compatible with the SIEM and properly configured to contain the necessary auditable events. Configuration must ensure that sufficient content of information is contained in the audit record. The types of events that are recorded in the assets audit log should be carefully planned and implemented across all assets. Auditing too much information can slow down the performance of the asset and create performance problems on the SIEM as well as negatively impact storage of the audit data.

Storage Requirements

A baseline for SIEM storage should be sized based on the expected daily audit log input times the minimum amount of time required to keep audit logs. Audit logs can increase dramatically during cyber events so it is important to remember this is only a minimum baseline. Expected growth of the infrastructure and possible expansion of regulatory audit requirements should also be considered when determining storage size. Confidentiality and integrity of the data must also be considered. Ensuring the data is unaltered and secure is vital for cyber incident event investigations.

Reporting

The SIEM analyzes audit logs looking for potential cyber events from single logs sources and by correlating events from all the log sources. Reports can be automated into daily reports or even alerts that are sent out to notify personnel of possible cyber events. Reports are a powerful tool aiding in audit compliance as well as identifying cyber event trends.

A SIEM can be a valuable tool for meeting audit requirements. Careful planning must be performed when determining the SIEM solution and how to integrate the solution into the infrastructure. The SIEM is only part of the auditing solution as consideration must be made for the existing infrastructure, regulation, and potential growth.

This month's contributor to Consultant's Corner is
Stephen Santee, CISSP, CISM, PMP
Consultant, Critical Infrastructure & Security Practice, Invensys
Stephen.Santee@invensys.com

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
June 2013 / Issue 21

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 Critical Infrastructure Consulting include:

Hardware Independence

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

Regulation Knowledge

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

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

Industry Knowledge

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

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 Assessments, Development, Implement and Management.

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**