June 2012 / Issue 09

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Compliance vs. Cyber Security

June 2012
Cyber Attack Statistics
- Hackmageddon.com

Attack Motivations
- 82% Cyber Crime
- 14% Hacktivism
- 4% Cyber Espionage

Top 3 Attack Targets
- 19% Industry
- 15% Government
- 10% Education

Top 5 Attack Techniques
- 42% Unknown
- 36% SQL
- 10% DDoS
- 8% Account Hack
- 1% DNS Poisoning

Trying to understand the difference between compliance solutions and cyber security solutions can be very confusing. Sir Walter Scott said it best: "Oh what a tangled web we weave." Every discussion on cyber security is interlaced with compliance elements and cyber security solution features. This is just compounded by the number of standards on the topics that primarily address compliance, so it is no wonder that many people confuse being cyber security compliant with being cyber secure. Cyber security compliance, while complimentary to cyber security solutions, is *not* cyber secure.

What is compliance? Compliance is defined by the laws, regulations, and governing bodies. These standards generally contain a list of "Requirements" that must be met in order to declare the user as "Compliant." Furthermore, being compliant requires the processes, tools and organizations to sustain the program in a manner that can be audited. In short, you must be able to display the actions and evidence required to show you meet the requirements.

Compliance Solutions
- Gap Analysis
- Compliance Status
- Audits
- Objective Evidence

Any comprehensive cyber security initiative begins with a compliance program and is monitored throughout its lifecycle. When executed properly, the outcome of the compliance program is the remediation checkpoints that drive the cyber security solutions.

The compliance process provides an overview of gaps and statuses as set forth by the regulation used (i.e. NERC-CIP, NEI 0809). This information is used to define assets that will need to be secured within the infrastructure and the extent of the security controls that must be applied. The deployment of the required security controls should always adhere to cyber security best practices.

Cyber Security Solutions
- Administrative Controls
  - Policies
  - Procedures
- Technical Controls
  - AV
  - Back Ups
  - Logging/Monitoring
  - Etc.

The deployment of cyber security solutions alone will almost never provide compliance to modern cyber security compliance standards, and neither will being compliant to the standard make you 100% secure. True security is a comprehensive program of compliance, cyber security solutions, and an organizational awareness of the risks and benefits of the technologies deployed in our modern industrial control systems.

Industry News

Hacker charged for breaching the U.S. Energy Department

HackerNews.com, 6/12/2012

A 23-year-old resident of Devon, Pennsylvania was arrested on Thursday and charged with one count of conspiracy, two counts of computer fraud, and one count of access device fraud, according to a statement issued by the Justice Department's Criminal Division. According to the indictment, between 2008 and 2011, Miller and others allegedly remotely hacked into computer networks belonging to RNK Telecommunications Inc., a Massachusetts company; Crispin Porter and Bogusky Inc., a Colorado advertising agency; the University of Massachusetts; the U.S. Department of Energy; and other institutions and companies. After gaining unauthorized access to these systems, Miller is alleged to have installed Trojan horse programs that gave him access to the networks, which he and his co-conspirators sold online. Miller and his co-conspirators were discovered after they attempted to sell access to the victim networks to an undercover FBI agent.

Disaster awaits U.S. power grid as cyber security lags

CNET.com, 6/14/2012

Security technology used by U.S. electric utilities is flawed and could increase the odds of computer intrusions or sabotage, the chairman of an industry standards group warns. Jesse Hurley, co-chair of the North American Energy Standards Board's Critical Infrastructure Committee, says the mechanism for creating digital signatures for authentication is insufficiently secure because not enough is being done to verify identities and some companies are attempting to weaken standards to fit their business models. "These certificates protect access to control systems," Hurley told CNET. "They protect access to a $400 billion market. They protect access to trading systems. They also protect access to machines that do things like turn generators off. If you issue a fraudulent certificate or you're lax... the consequences could be disastrous." The U.S. electrical grid has already become a target of cyber attacks, with Chinese and Russian hackers reportedly penetrating it over the Internet.

Nuclear regulator warns about cyber security lapses at California power plant

Infosecurity-magazine.com, 6/15/2012

The U.S. Nuclear Regulatory Commission (NRC) is warning Southern California Edison that it might take enforcement action against the utility because of cyber security lapses found in a May security audit of its San Onofre nuclear power plant. In a letter to Southern California Edison, the NRC said that the utility failed to "develop a site procedure which addressed the need to conduct a cyber security analysis of electronic devices designated for safeguards information" at the plant, according to a copy of the letter obtained by the North County Times newspaper. According to the NRC website, "safeguards information" is a "special category of sensitive unclassified information…to be protected" concerning the "protection of operating power plants, fuel shipments, strategic special nuclear material or other radioactive material." The NRC acknowledged that the utility had fixed the cyber security lapses at the plant, but it is still considering enforcement action.

Utility regulators investigating preparedness for cyber attacks

courierpress.com, 6/9/2012

INDIANAPOLIS — State utility regulators plan to investigate during a series of meetings in the coming months of whether Indiana's power companies are adequately prepared to combat cyber attacks. Indiana Utility Regulatory Commissioner Carolene Mays provided a peek at the concerns last week when she asked the companies—which were gathered for a forum to talk about the summer cooling season—about the issue. Mays serves as vice chair of the National Association of Regulatory Utility Commissioners' Committee on Critical Infrastructure and said concern about cyber hackers keeps her up at night. "It's one of our major focuses right now because utilities across the country are just not prepared," Mays said. "Nationally, they're proving they're not prepared for potential cyber security issues." If hackers break through an electric provider's network security, they could have the power to stop energy transfer to entire cities.

Cyber News

Microsoft security system compromised, potential collateral damage from Flame virus

ABC News, 6/4/2012

Microsoft revealed that the Flame virus compromised a "key Microsoft security system," forcing the company to release an emergency patch to millions of customers whose systems may have been affected. Microsoft told its customers that authors of the Flame virus had been able to infiltrate Microsoft's security system and "forge digital security certificates, which then allows the malicious code to spread undetected by anti-virus programs." Though Microsoft fixed the breach, it was considered to be a glimpse of the collateral damage likely to be caused by the Flame virus attacks on Iran's nuclear programs. "This may be an example of how U.S. and Israeli cyber war has the blowback effect that threatens the security of American networks," said Richard Clarke, former White House counter-terrorism advisor and ABC News consultant. When Microsoft announced its security breach, the Israeli military immediately claimed they have "been engaged in cyber activity consistently and relentlessly, gathering intelligence and defending its own cyber space."

U.S. and Israel involvement in Flame virus confirmed

RT.com, 6/20/2012

Western officials confirmed that the United States and Israel worked together to develop the Flame virus. According to officials, "the CIA, National Security Agency (NSA), and the Israeli military were all involved in developing malware to sabotage Iran's nuclear program." Flame began cyber attacks on Iran's oil ministry and export facilities by "activating microphones and cameras, taking screenshots, logging keyboard strokes, extracting geolocational data from images and sending and receiving commands via Bluetooth wireless technology." Kaspersky Lab, a Russian cyber security firm, determined the virus' malicious code to be eerily similar to that of Stuxnet, a virus that the U.S. government had been suspected of creating, and concluded that they were "100 percent sure that the Stuxnet and Flame groups worked together." Stuxnet targets Siemens software and equipment, which is incidentally what Iran uses for its nuclear enrichment facilities. Flame has been noted as one of the most serious threats experts have ever come across.

How Flame malware fakes Microsoft Windows

ComputerWorld.com, 6/18/2012

Security researchers have determined that Flame malware infiltrates fully patched Windows 7 computers by exploiting Microsoft's Windows Update feature. According to researchers, "hackers had located and exploited a flaw in Microsoft's Terminal Services licensing certificate authority that allowed them to generate code-validating certificates 'signed' by Microsoft." With fake certificates, attackers were able to trick Windows 7 PCs into accepting a malicious file as a Microsoft update. However, rather than infiltrating Windows Update to send malicious files to users, "a rogue configuration file modifies a machine's settings to route all traffic through the Flame-infected system, creating a complex mechanism for spreading the malware." Microsoft has been working to combat the virus.

The future of Flame

The Globe and Mail, 6/22/2012

In the aftermath of the Flame cyber attacks last April, Iran complained about a new cyber threat, saying it "had detected plans by the United States, Israel and Britain to launch a 'massive' strike after the breakdown of talks over Tehran's nuclear activities." Whether the threat referred to the Flame virus or a new virus was unclear. Many experts on cyber warfare believe Flame could be used in the future to sabotage critical infrastructure, including dams and chemical plants.

Consultant's Corner

AWWA ACE12 — Dallas, TX June 10-13, 2012

The AWWA annual conference for 2012 has come and gone. It was a great conference in many respects this year: It was held in my home state of Texas, it was the first year we had a cyber security presence in our booth, I participated in my first standards committee meeting as a voting member, and we started reviewing the ANSI/AWWA G430 "Security Practices for Operation and Management" standard.

Cyber security and water are two words I would have never thought would appear in the same sentence, given my background in process controls and the many times I've been at some remote well site with nothing but a chain link fence and a pad lock between me and the PLC (which I could access wirelessly) that operated the site. Then, on that fateful day of September 11, 2001, everything changed. Homeland Security Presidential Directive-7 identified the *"Critical Infrastructure and key resources which provide the essential services that underpin American society."* One of the eighteen was drinking water and waste water treatment systems. In response, the Water Sector Coordinating Council Cyber Security Working Group (sponsored by American Water Works Association and the Department of Homeland Security) released the "Roadmap to Secure Control Systems in the Water Sector" in March 2008. This document captured many findings and recommendations and is one of the driving factors behind the development of the ANSI/AWWA G430 standard. In my opinion, we are still in the phase of educating the industry about cyber security, its value, and the potential consequences of ignoring it.

As late as last year (coincidently over the September 11th weekend) at the 2011 Water Security and Emergency Preparedness Conference in Nashville, TN, I saw hardly any cyber security representation. Security was still identified as fences, locks, cameras, contamination monitoring—anything to physically keep the bad guys out. There was little attention paid to that PLC behind the fence that was now directly accessible from the internet. I'm glad to say that I think things are definitely changing. I've had several opportunities to speak at regional AWWA/WEF events about cyber security and I managed to volunteer for the standards committee. Enquiries from water and wastewater clients are increasingly concerned about cyber security. This year is looking bright; we just finished up the AWWA annual conference, the standard draft is making its rounds, I've had conversations with high-level members of AWWA saying that cyber security is a major initiative, and I'm on the schedule to present at the 2012 Water Security and Emergency Preparedness Conference "Best Practices in SCADA Cyber Security."

I look forward to seeing all of you in St. Louis, MO September 9-12, 2012.

This months contributor to Consultant's Corner is
Michael Martinez
Principal, Critical Infrastructure & Security Practice
Invensys
michael.martinez@Invensys.com

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
June 2012 / Issue 09

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**