November 2011 / Issue 02

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

- Water Treatment Security
- Industry News
- Consultants Corner
- Invensys CISP News

Focus on Water Treatment

Dept. of Homeland Security (DHS) 2003
Presidential Directive 7 (HSPD7) Water is a Critical Infrastructure

EPA 2008
National Infrastructure Protection Plan for Water

Water Treatment Facilities
Urban Providers >4,000
Rural Providers >50,000
(source EPA)

Wastewater and Water Treatment Critical Cyber Security News

This past month saw two Water Treatment facilities report possible security breaches of their control networks. Although the incident in Illinois was determined to be a false positive, the Texas incident appears to be a legitimate network hacking. In either case there is a strong lesson to learn. In either case, a person intentionally or unintentionally took advantage of a simple security lapse. The Illinois breach could have been prevented through secure remote data acquisition. The Texas hack appears to be due to a lack of strong passwords and the discipline to manage passwords system wide, do not keep the administrator default.

Water Treatment in the News

Hacker says he broke into Texas water plant, others

- From CNET.com 11/18/2011

A twenty something hacker said today that he hacked into a South Houston water utility to show that it can easily be done, after U.S. officials downplayed the risks from a report yesterday of an intrusion at an Illinois water plant. The hacker, using the alias "pr0f," said he has hacked other SCADA (supervisory control and data acquisition) systems too.

DHS sees no evidence of Cyber attack on Ill. Water facility

- From Network World 11/23/2011

The U.S. Department of Homeland Security (DHS) today said there is nothing to suggest that a recent pump failure at a Springfield, Ill. water utility was caused by a cyber attack as previously reported by an industrial control systems security expert.

Industry News

Water System Hack—The System is Broken - *From ControlGlobal.com 11/17/2011*

Last week, a disclosure was made about a public water district SCADA system hack. There are a number of very important issues in this disclosure:

- The disclosure was made by a state organization, but has not been disclosed by the Water ISAC, the DHS Daily unclassified report, the ICS-CERT, etc. Consequently, none of the water utilities I have spoken to were aware of it.
- It is believed the SCADA software vendor was hacked and customer usernames and passwords stolen.
- The IP address of the attacker was traced back to Russia.
- It is unknown if other water system SCADA users have been attacked.
- Like Maroochy, minor glitches were observed in remote access to the SCADA system for 2-3 months before it was identified as a cyber attack.
- There was damage – the SCADA system was powered on and off, burning out a water pump.

French Nuclear Power Company Hit by Cyber Attack - *From eSecurityPlanet.com 11/2/2011*

French energy conglomerate Areva may have been hit by an attack first detected in September. "Local reports are consistent only in terms of talking about cyber-espionage, perhaps involving malware rather that some kind of terrifying Stuxnet-style nuclear kit sabotage caper"

US vulnerable to cyber attacks: military chief - *From Reuters 11/28/2011*

The top U.S. military officer said on Monday the United States was vulnerable to cyber attacks, and called for more aggressive action to bolster America's online defenses.

The comments by General Martin Dempsey, chairman of the Joint Chiefs of Staff, were the latest by U.S. military officials flagging cyber security as an area of growing focus and investment even as the Pentagon braces for declining budgets.

Coordinated Cyber Attacks Hit Chemical and Defense Firms - *From SecurityWeek.com 10/31/2011*

Attackers have been targeting chemical and defense companies around the world in a cyber campaign designed to steal information. The attacks have been dubbed 'Nitro' by Symantec, which released a whitepaper on the situation earlier today. In late July, the attackers moved on to the chemical industry and began targeting 29 companies. At least 48 companies are believed to have been targeted.

U.S. Report warns of cyber spying by Russia, China - From InfoWorld 11/3/2011

Espionage attempts are expected to increase as more sensitive information moves online in areas such as pharmaceuticals, defense, and manufacturing. The U.S. can expect more aggressive efforts from countries such as Russia and China to collect information through cyber espionage in areas such as pharmaceuticals, defense, and manufacturing, according to a new government report released Thursday.

Consultants Corner

Tim Johnson, CISSP —CISP Principal Consultant

"Centralized Anti-virus DAT repository deployments enable quick and reliable Anti-Virus updates for Stand Alone Control Systems."

Doug Clifton, CISSP — Dir. CISP

"Its significantly less expensive to purchase Managed Security Services than hire new staff with Security Experience. Are you in control of the USB drives at your site."

Steve Batson — CISP Principal Consultant

"Implementing common security controls across disparate systems can greatly reduce the cost of security and maintenance."

Michael Martinez — CISP Principal Consultant

"Being regulatory compliant does not ensure being secure. Cyber Security is a on going life cycle"

Tom Jackson — CISP Principal Consultant

"According to Kaspersky Labs, applications like Adobe are primary targets for hackers to deliver viruses. Implementing patch management and update services is an effective fix"

Meet the CISP team and learn more about Cyber Security at http://www.real-time-answers.com/cyber-security/

Cyber Security for the Nuclear Industry »
Focusing on 10 CFR 73.54 and NEI 08-09 Reg. guide 5.71, learn more about cyber security in the nuclear industry.

Cyber Security for Power Generation »
As more and more electric power plants begin their NERC CIP compliance plan, many are left trying to understand where to start. See which areas require special attention.

Cyber Security Compliance »
Cyber compliant does not necessarily mean cyber secure. Identify the keys common to both.

Cyber Security Threats »
Cyber attacks are increasing. A continuous state of preparedness is required.

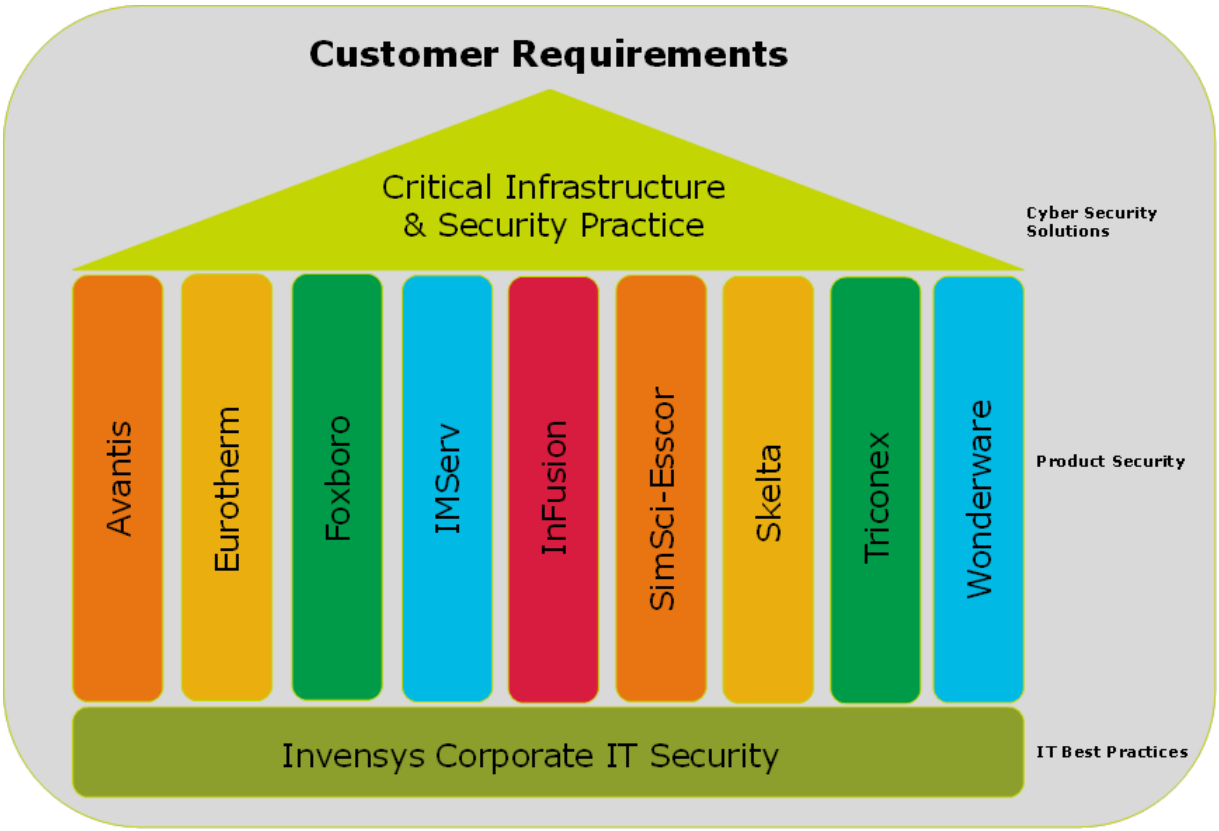
Cyber Security Life Cycle »
Cyber security cannot be maintained from a one-time initiative. Learn about a methodology designed to keep your site cyber secure well into the future.

Cyber Security Consulting Advantage »
Security and compliance take a tremendous amount of effort. Help is available to get secure and compliant … and stay that way.

CISP DNA

CISP Cyber Security DNA

At Invensys, security is a primary focus to all development efforts ensuring that we meet our customer's requirements. The Critical Infrastructure & Security Practice (CISP) builds on the firm corporate IT security practice and the cross portfolio product security development, delivering complete integrated security solutions and security programs for our clients entire plant and infrastructure. With this alignment it ensures that our Cyber Security solutions reflect the best Invensys has to offer
The CISP team has years of specialized Cyber Security experience and extensive industry knowledge. When combined, CISP can deliver Cyber Security solutions for any regulatory or industry requirement facing customers today.



Invensys CISP News

Invensys Critical Infrastructure and Security Practice News and Events

NERC-CIP Requirements Show Cybersecurity's Future

- From ControlGlobal.com 11/09/2011

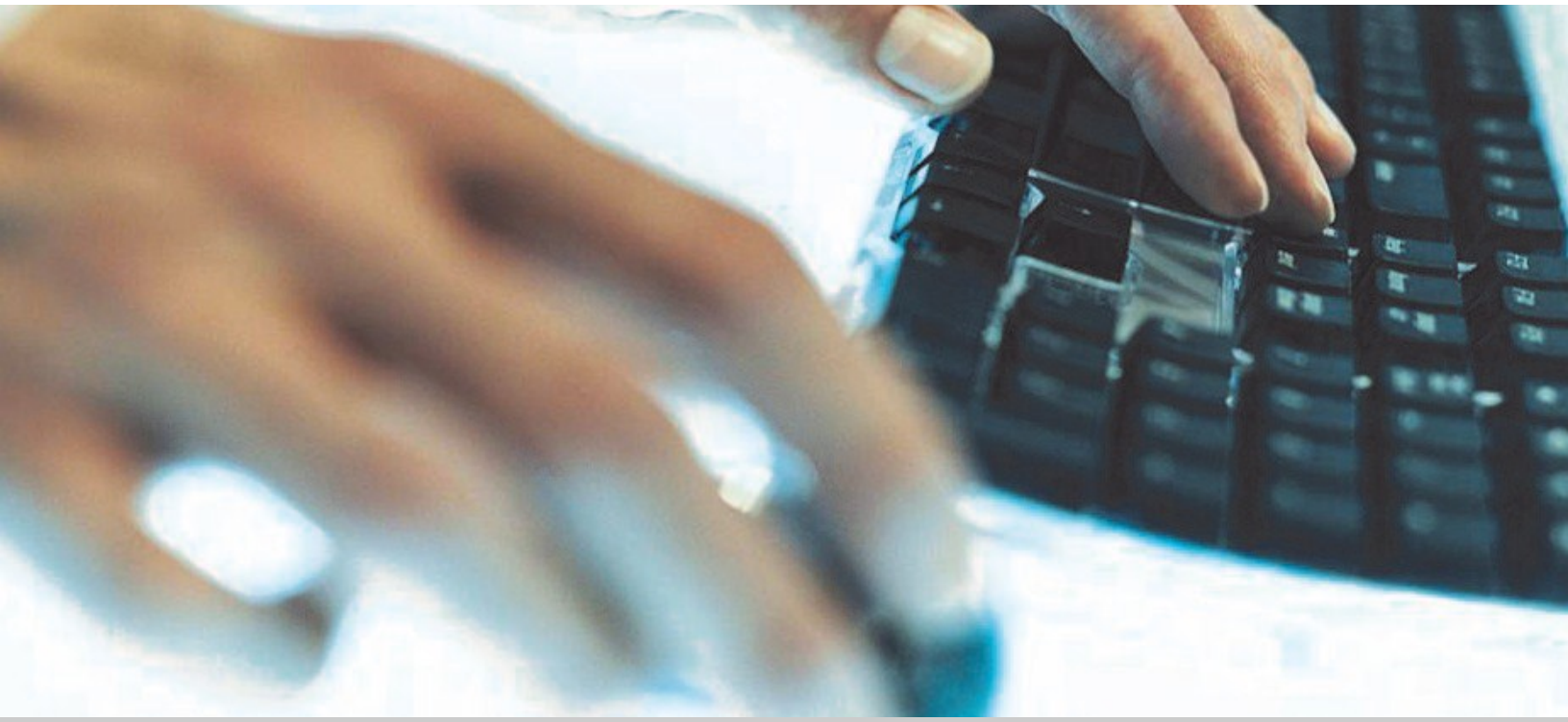
Cybersecurity is no longer a stranger. It's just another pillar of operational excellence at Invensys Operations Management, much like its well-known "environment and safety," "people," "asset" and "control" cornerstones. And so, wisely making cybersecurity familiar and approachable may be exactly what's needed to take it on and get it done.

Michael Martinez, principal consultant for critical infrastructure and security at Invensys, reports there are several primary drivers for cybersecurity in control systems. "Control networks are no longer islands, and they're using commercial off-the-shelf technologies (COTs). However, this also makes them subject to the same vulnerabilities as COTs, such as the cyber-attacks and viruses like Stuxnet that are such big news," explained Martinez.
See the entire article at http://www.controlglobal.com/articles/2011/opsmanagement11-17.html

UPCOMING: AWWA March 2011 Michael Martinez-Principal Consultant to present on SCADA Security

- Abstract

Supervisory Control And Data Acquisition (SCADA) systems are used throughout the Water and Wastewater industry to monitor and control the processes which allow them to provide reliable affordable high quality water and services to their customers. In 2003, the Homeland Security Presidential Directive 7 (HSPD7) identified Water as one of its critical infrastructures.



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.

Industry Knowledge

CISP has a number of resources that understand the demands of Controls 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 active participation 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 Assessments, Development, Implement 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.

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**