February 2012 / Issue 05

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Threat Report - McAfee

- Total Malware in 2011 exceeded 75 million
- Malicious sites doubled

Mobile Threats - Juniper

- Android Malware grew by 3,325% in just 7 months
- Malware types: Spyware 63% SMS Trojans 36%

Cyber Security Market — Info Security

- Global market will reach $80 Billion by 2017

Government Weighs In on Cyber Security

Don't look now, but the number of cyber security regulations for U.S. businesses and industries is about to increase as Washington DC looks to pass more cyber security legislation, although the specifics of "when" and "how" are not completely clear. The federal government is very focused on cyber security and with a good reason if the last couple of years has taught us anything. The Cyber Security Act of 2012 (S. 2105) was introduced on Feb. 14. The proposed bill would have the Department of Homeland Security (DHS) create a program for cyber security research and development and stand up a process for designating high-priority critical infrastructure, assessing its risks and building a regulatory framework for setting and enforcing cyber security standards. The bill says DHS should work with various industry groups and government agencies to set cyber security standards for covered critical infrastructure. Self-reporting would be the primary oversight mechanism and DHS would determine penalties for not meeting security standards. This Senate bill is viewed as having more regulatory "teeth" than the House Homeland Security proposal, H.R.3674, as far as incentives and penalties are concerned.

Also, keep in mind that on October 12, 2011, the Securities Exchange Commission (SEC) introduced Corporate Finance Disclosure Guidance with regards to cyber security. The SEC says "a company probably will need to report on costs and consequences of material intrusions in which customer data are compromised." The company's revenue could suffer, and it could be forced to spend money to beef up security or fight lawsuits. In addition, if a company is vulnerable to cyber attacks, investors may need to be informed of the risk, the SEC says. So how does this impact Industrial Control Systems (ICS) today? One thing is certain: cyber security regulations are no longer a plant control system issue lacking visibility and support. The impact of cyber security regulations will now be felt from the board room to the control room. Responsibility is now a corporate issue impacting the CEO, CFO, and CIO all the way to the Process Engineer.

Gov't Cyber News

DHS takes the lead in Senate cybersecurity bill - *From FierceGovernmentIT.com 02/22/2012*

Newly-introduced cybersecurity legislation would task the Homeland Security Department's national cybersecurity and communications integration center with facilitating information sharing among public and private-sector entities, rather than creating an industry-controlled, non-profit National Information Sharing Organization, as suggested by one proposal in the House. The Cybersecurity Act of 2012 (S. 2105) would also have DHS create a program for cybersecurity research and development and stand up a process for designating high-priority critical infrastructure, assessing its risks and building a regulatory framework for setting and enforcing cybersecurity standards.

Senators introduce new cybersecurity bill - *From CNET.com 02/14/2012*

DHS would decide what firms are "critical infrastructure" and require them to meet security standards. The Cybersecurity Act of 2012 calls for the DHS to assess risks and vulnerabilities of computer systems running at critical infrastructure sites such as power companies and electricity and water utilities and to work with the operators to develop security standards that they would be required to meet.

White House proposes Consumer Privacy Bill with Do Not Track - *From THSecurity.com 02/24/2012*

A white paper has been released by the U.S. government proposing a new "Consumer Privacy Bill of Rights" and, as part of the proposals, the use of "Do Not Track" technology is to be enshrined in law. In making the announcement, President Obama said "As the Internet evolves, consumer trust is essential for the continued growth of the digital economy. That's why an online privacy Bill of Rights is so important." Alongside the white paper, the Digital Advertising Alliance (DAA) announced that member companies including Google, Yahoo!, Microsoft and AOL have agreed to comply when consumers use "Do Not Track" technology in their browser. "Do Not Track" allows users to set in their browser an indication that they do not want to be tracked through the use of cookies or other mechanisms. The companies that have agreed so far account for nearly 90% of online behavioral advertising. The White House added that having agreed to the "Do Not Track" commitment, those companies will be subject to enforcement by the FTC. "Do Not Track", as proposed by Mozilla in January 2011, was passed to the W3C for standardization, though this process is still ongoing.

2013 Federal Budget Includes Nearly $800MM for Cybersecurity - *From ThreatPost.com 02/14/2012*

President Obama is asking for $769 million to fund information security initiatives via the Department of Homeland Security in 2013. That amount is nearly twice what DHS asked for last year to fund its cybersecurity work. "The Administration proposes $769 million to support the operations of the National Cyber Security Division, which protects Federal computer systems and sustains efforts under the Comprehensive National Cybersecurity Initiative to protect U.S. information networks from the threat of cyber attacks or disruptions. The benefits of this investment extend beyond the Federal sphere and will help strengthen state and local governments' and the private sector's capabilities to address cyber threats," the budget request says. The money for the DHS cybersecurity efforts is just one component of the budget that is involved with the country's programs for information and network security.

Industry News

Keeping the Lights On In The Face of Cyber Attacks - *From Securityweek.com 02/21/2012*

The shift from proprietary control systems to distributed systems built with commercial, off-the-shelf software has changed the name of the game and the "security by obscurity" approach no longer works. The probability of being able to penetrate or attack systems is far greater than ever before. With utility companies powering so much of the critical infrastructure, from transportation, water, and telecommunications to financial services—a disruption to the supply and distribution of electricity would affect virtually everything.

Scared of Anonymous? NSA Chief says you should be - *From CNET.com 02/21/2012*

According to the Wall Street Journal, Gen. Keith Alexander has said in private meetings at the White House and elsewhere that the U.S. must keep a close eye on Anonymous' growth. He reportedly warned that if the organization continues to gain power, it might even take down a part of the U.S. power grid within the next couple of years. How serious might such an attack on the power grid be?

Nuclear plant safety report on USB stick lost by official - *From Techworld.com 02/17/2012*

The report on Hartlepool nuclear power station was reportedly downloaded in unencrypted form onto the drive before being lost by a senior Health and Safety Executive (HSE) official while at a conference in India, sources told The Sun newspaper. Containing extensive technical plans to the EDF-owned plant, the report was part of an assessment carried out on all ten of the country's nuclear power stations in the aftermath of the Fukushima incident after the Japan Tsunami last March. "The use of unencrypted USB pen drives is not permitted by ONR for transporting documents with a security classification," an official confirmed.

Chemical Facility Security News - *From ICS.com 02/14/2012*

Cybersecurity Act of 2012 and ICS Security Sen. Lieberman (I,CT) {along with co-sponsors Collins (R,ME), Rockefeller (D,WV) and Feinstein (D,CA)} introduced S 2105, the Cybersecurity Act of 2012; the long awaited and much anticipated comprehensive cybersecurity bill. In no surprise to anyone that has been paying attention, the bill never mentions industrial control systems or any of their components. There are provisions, however, that may have an impact on how the federal government deals with control system security issues.

New Tool Will Automate Password Cracks on Common SCADA Product - *From ThreatPost.com 02/08/2012*

The fallout from last month's S4 Conference continues in February, with a planned Valentine's Day release of tools that make it easy to test and exploit vulnerable programmable logic controllers and other industrial control systems. Among the releases will be a tool for cracking passwords on the common ECOM programmable logic controllers by Koyo Electronics, a Japanese firm.

Iran: Nuclear facilities immune to cyber attacks - *From YahooNews.com 02/13/2012*

TEHRAN, Iran – A senior Iranian military official said Monday that Tehran's nuclear and other industrial facilities suffer periodic cyber attacks, but that the country has the technology to protect itself from the threat, an official news agency reported. Jalali said that in addition to Stuxnet, Iran has discovered two espionage viruses, Stars and Doku, but that the malware did no harm to Iran's nuclear or industrial sites.

Cyber News

Hackers claim to have intercepted call between FBI, Scotland Yard - *From FoxNews.com 02/03/2012*

A sensitive conference call between the FBI and Scotland Yard was recorded and released online by the hackers in Anonymous, the group claimed Friday. The group released a roughly 15-minute long recording of what appears to be a Jan. 17 conference call devoted to tracking and prosecuting members of the loose-knit hacking group. The authenticity of the recording could not be immediately verified and it's unclear how the hacking group obtained it. Names of some of the suspects being discussed were apparently edited from the recording. The information was illegally obtained and a criminal investigation is underway.

Hackers intercepted FBI, Scotland Yard Call - *From AP.com 02/03/2012*

Unfortunately for the cyber sleuths, the hackers were in on the call too—and now so is the rest of the world. Anonymous published the roughly 15-minute long recording of the call on the Internet on Friday, gloating in a Twitter message that "the FBI might be curious how we're able to continuously read their internal communications for some time now." The humiliating coup exposed a vulnerability that might have had more serious consequences had someone else been listening in on the line.

Nearly 80% of All Bugs Are In Third-Party Apps - *From DarkReading.com 02/14/2012*

Don't blame it on Microsoft: The lion's share of vulnerabilities last year were in third-party applications, with 78 percent of all bugs, versus 10 percent in Microsoft software products, according to a new report published. Secunia's annual report for 2011 found that the number of endpoint flaws jumped past 800 bugs, more than half of which were considered very critical. "What we see is a consolidation, with fewer vendors responsible for more vulnerabilities," says Stefan Frei, research analyst director for Secunia. "Most of the vulnerabilities are highly critical and exploitable." The jump in third-party flaws is dramatic when compared with 2006, when it was less than half, at 45 percent. Around 12 percent of last year's bugs were in operating systems.

Got remote access? Lock it down - *From InfoWorld.com 02/10/2012*

Remote-access software led to a stunning 62 percent of breaches studied by security firm Trustwave in its recently released global security report. The company looked at 300 breaches it investigated on behalf of clients and analyzed the results of 2,000 penetration tests. The company found that hacking accounted for half of all breaches, and 64 percent of those hacks exploited weaknesses in remote-access software.

Nortel Networks: Wolf In The Henhouse, Guard Dog Fast Asleep - *From DarkReading.com 02/17/2012*

If you're a wolf that wants to go undetected in hunting for hens or their eggs on a midnight raid of Farmer Brown's nearby chicken coop, you generally have only two choices. Try slipping by the sleeping guard dog and hope you don't get caught, or walk right up to and past his vigilant counterpart, all the while knowing full well he's not going to wake the sleeping farmer. That's the analogy summoned in reading about the recent Wall Street Journal report that hackers, reportedly from an IP address located in China, breached bankrupt Nortel Networks security as far back as 2000 and stole seven passwords from the company's top executives—including the CEO—which granted them widespread access to the entire Nortel network. Shields, who worked for Nortel for 19 years, claims that the company discovered the hack in 2004 when it was determined that some PCs were regularly sending sensitive data to an IP address based in Shanghai.

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

"It's significantly less expensive to purchase Managed Security Services than to hire new staff with Security Experience."

Steve Batson, CISSP — 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 ongoing 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.

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 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 help them 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 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.

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**