September 2012 / Issue 12

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

Our plant has been hacked!

This headline is showing more and more as of late. Over these past months we have read about cyber security incidents at water plants, pipelines, power plants and oil-gas refineries. This has been a growing trend across all industries, however the Energy sector has found itself with the bulls eye on its back as of late. And for good reason—the industry's vast number of digital control systems (DCS) make ideal targets of opportunity if left unprotected.

The Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) recent report for 2009-2011 details some interesting facts:

- Cyber incidents up 383% in 2011 from 2010
- Water and Energy sectors reported highest
- Water was 41% of reported incidents
- Energy was 16% of reported incidents
- Government facilities made up 6% of reported incidents

There are a number of contributing factors today that were not available ten or twenty years ago. The price of a basic PC was a simple barrier to access for the majority of people, and coupled with lack of Internet access, there were fewer cyber crimes ten years ago. Fast forward to 2012: 75% of households in the industrialized world have PCs and access to the internet, which has opened a whole new channel for hackers and individuals looking to be hackers. Root kits, or cyber hacking kits with well-developed user interfaces, are readily available on the web for as little as $200 USD. For relatively little money, a would-be cyber criminal anywhere in the world is in business and capable of devastating a company's digital assets. The lower cost barrier has ushered in new breeds of hackers. There are now Hacktivists, socially and politically motivated groups who target specific companies based on a profile, looking to gain recognition. These groups can also work collectively against a common target. Nation-states, on the other hand, hide in the shadows. These are foreign countries, typically China and Russia, carrying out espionage in a very sophisticated manner. They tend to target military and critical infrastructure (power, water, pipelines) within the U.S. Their intent is not clearly understood; however, they have proven to be relentless in probing targets within the U.S.

Just as important as preparing for a cyber attack is the preparation for a cyber incident after the attack has occurred. Bill Owen, Principal Consultant on the Invensys Nuclear Cyber Security team, has written an article for this month's Consultant's Corner, "Nuclear Incident Response," addressing how the Nuclear industry responds to such a cyber event.

Getting hacked was once viewed as a matter of "if," not "when." Today, a cyber attack is much more a matter "when."

Sept. 2012
Cyber Attack Statistics
- Hackmageddon.com

Attack Motivations
56% Cyber Crime
44% Hacktivism

Top 3 Attack Targets
30% Government
16% Industry
10% Organizations

Top 5 Attack Techniques
48% SQL
19% DDoS
19% Unknown
8% Java Vulnerabilities
3% DNS Hijacking

Industry News

Saudi Aramco hacked
Gas2.org, 9/2/2012

Saudi Aramco, the world's largest oil-producer, was hit by a malevolent computer virus in late August, which crippled nearly 30,000 of the company's workstations and threatened to permanently delete most of the company's electronic data. This, by the way, comes directly from Saudi Aramco representatives, who revealed that the virus "originated from external sources," and that its private investigations into the matter were ongoing. Saudi Aramco has restricted ALL inbound electronic access, which includes email, apparently, as Reuters reported that it attempted to reach out to the company further but saw its e-mails bounced back.

Cyber attack takes Qatar's RasGas offline
arabianBusiness.com, 9/1/2012

RasGas, the second largest producer of Qatari LNG after Qatar Petroleum, has been hit with an "unknown virus," which has taken the company offline. A RasGas spokesperson confirmed that "an unknown virus has affected its office systems" since Monday, August 27. RasGas confirmed the situation by fax yesterday. "RasGas is presently experiencing technical issues with its office computer systems," said the RasGas fax seen by Oil & Gas Middle East, dated August 28. "We will inform you when our system is back up and running." The RasGas spokesman said the virus has "no impact whatsoever on operations in Ras Laffan Industrial City and there are no issues with cargo deliveries."

Cyber espionage campaign targets oil companies
SecurityWeek.com, 9/20/2012

Researchers from Dell SecureWorks' Counter Threat Unit say they have discovered yet another cyber espionage campaign targeting oil and energy companies. Its targets, they say, include a large oil company in the Philippines, an energy company in Canada, a military organization in Taiwan, and other organizations in Brazil, Israel, Egypt, and Nigeria. "Based on the data collected by the CTU research team, the campaign's primary attack vector is spearphishing emails that target mid-level to senior-level executives," blogged Silas Cutler of Dell SecureWorks Counter Threat Unit, Threat Intelligence. "These emails contain an attachment that includes a malicious payload that installs a copy of Mirage." The "weaponized" attachments are designed to look like PDF files but are actually "droppers" —standalone executable files that open an embedded PDF file and execute Mirage, Cutler explained.

Danger from the Internet: Cyber attacks on energy grids
Wire-Tradefair.com, 9/2012

Luckily so far no critical energy infrastructure installations like electricity supply, gas and oil networks, coal-fired and nuclear power stations, or regenerative energy operations have been damaged by computer attacks. However, energy grid operators see the risk of digital attacks as a growing problem.

U.S. says natural gas pipelines under cyber attack
Emergencyemail.org, 9/24/2012

The country's Homeland Security agency said Tuesday the attacks involve "sophisticated spearphishing —fake emails that appear to be legitimate to employees at the natural gas companies"—designed to try to get them to divulge passwords or other secure information.

Canada warns that Anonymous may attack Oil Sands energy companies
OilPrice.com, 9/3/2012

According to documents that have recently been obtained by Bloomberg News this month, the Royal Canadian Mounted Police (RCMP), Public Safety Department, and Communications Security Establishment Canada, have all investigated threats that have been made against the Canadian oil industry by the Anonymous hacker group. Oil companies working in Canada's oil sands have been warned that they could face a cyber attack. "Anonymous has demonstrated that it can effectively mount cyber attacks with the potential to disrupt corporate or government operations." The report found that Anonymous has already infiltrated Toronto's police, the Bank of America Corp., and the Australian and Syrian governments.

Cyber News

Powerful cyber attack tools widely available, say researchers

ComputerWeekly.com, 9/3/2012

Online cyber criminal markets are putting very sophisticated attack tools into the hands of more low-level attackers, say cyber intelligence specialists. More attackers are now getting their hands on tools like Zeus and SpyEye, according to the cyber intelligence team at the Online Threats Managed Services (OTMS) group of RSA, the security division of EMC. Such tools are widely available at a relatively low cost, said Idan Aharoni, head of the cyber intelligence team for RSA's OTMS. The barriers to entry are falling all the time because these tools are also increasingly easy to use with well developed user interfaces, he told Computer Weekly.

Mobile malware is up—way up

ThreatPost.com, 9/4/2012

McAfee released its Q2 Threat Report, in which its researchers say they've unearthed 1.5 million new pieces of malware this year, or an average of nearly 100,000 malware samples a day. More and more malicious code is targeting Google's Android OS, though Apple users are far from immune too. More than 100 new Mac oriented samples were discovered last quarter. "In our 2012 Threats Predictions we predicted that this technique, likely inspired by the success of Duqu and Stuxnet, would rise in 2012. That opinion seems to be a successful example of crystal ball -gazing."

This week in cybercrime: Internet Explorer too dangerous to use?

Spectrum.IEEE.org, 9/22/2012

Internet security experts are warning computer users to avoid using Microsoft's Internet Explorer browser until a patch can be created for a vulnerability discovered last week. "There really isn't any great defense against [the exploit employed to take advantage of the flaw]," Johannes Ullrich, chief technology officer for the SANS Internet Storm Center, told Tech News World. According to Tech News World, On September 17, Microsoft issued an advisory noting that "an attacker could host a specially crafted website that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view the website."

Microsoft carries out Nitol Botnet takedown

ThreatPost.com, 9/13/2012

A botnet known as Nitol, built on the backs of PCs and laptops loaded with malware somewhere in the supply chain, was taken down by Microsoft. Microsoft's Digital Crimes Unit was given permission this week by the U.S. District Court for the Eastern District of Virginia to take over the 3322.org domain and more than 70,000 sub-domains hosting the Nitol botnet.

Flame analysis uncovers unknown malware, traces espionage tool back to 2006

SecurityWeek.com, 9/17/2012

According to research by Kaspersky Lab, Symantec, CERT-Bund/BSI, and the International Telecommunication Union's Impact Alliance, the development of Flame's command and control (C&C) platform began as early as December 2006. This is much earlier than researchers initially thought; the first reports placed Flame's development in 2010. Later, it was discovered that some domains used by Flame were registered in 2008. An analysis of the malware's C&C servers, however, revealed that developers had left internal timestamps and their nicknames in scripts.

Stuxnet tricks copied by computer criminals

TechnologyReview.com, 9/19/2012

Techniques used by government-backed malware are surfacing in the code used by ordinary cyber criminals. "They are copying the design philosophy," says Schouwenberg, adding that one now-popular technique found in conventional "criminal malware" was inspired by the discovery of Stuxnet.

Consultant's Corner

Nuclear Incident Response

A component of the Invensys Critical Infrastructure and Security Practice (CISP) is to offer Cyber Security Event and/or Incident Response support. This article is the first in a series meant to outline the rules, requirements, and standard methods for preparing for incidents and to provide methods for responding to actual events, including using appropriate processes to collect records via forensic analysis.

All nuclear power plants in the United States are regulated by the Nuclear Regulatory Commission (NRC) and are required to implement certain security controls. Any systems considered Safety, Security, Emergency Preparedness, and/or Support Systems (SSEP) are required by law (NRC 10.CFR.73.54) to have certain controls in place.

Cyber security programs at U.S. nuclear facilities are subject to 10.CFR.73.54, Protection of Digital Computer and Communication Systems and Networks, and must consider following Regulatory Guide (RG) 5.71, Cyber Security Programs for Nuclear Facilities, or an approved alternate method when implementing these programs. Accordingly, the Nuclear Energy Institute (NEI) developed an approved alternative to satisfy the rule, NEI 08-09 Revision 6: Operational, Management, and Security Controls. RG 5.71 and NEI 08-09 were both built on NIST 800-53 standards.

Cyber Security Plans (CSP) for all United States nuclear plants have been developed and the NRC has approved these plans. Section 4.6 of these Cyber Security Plans requires licensees to put in place a comprehensive Incident Response Plan (IRP). These plans are required to include processes to detect, deter, and respond to cyber attacks while mitigating the effects of the attacks and documenting forensic information (records) pertaining to the attacks if kept.

A cyber incident response capability must include several elements that are proactive in nature to prevent an incident or better allow the organization to respond when one occurs. These elements are green in Figure 1 and include planning, incident prevention, and post-incident analysis/forensics. Other elements center on detecting and managing an incident once it occurs. These are reactive in nature and are typically carried out under severe time constraints and great visibility. These elements, shown in red in Figure 1, include detection, containment, remediation, recovery, and restoration.

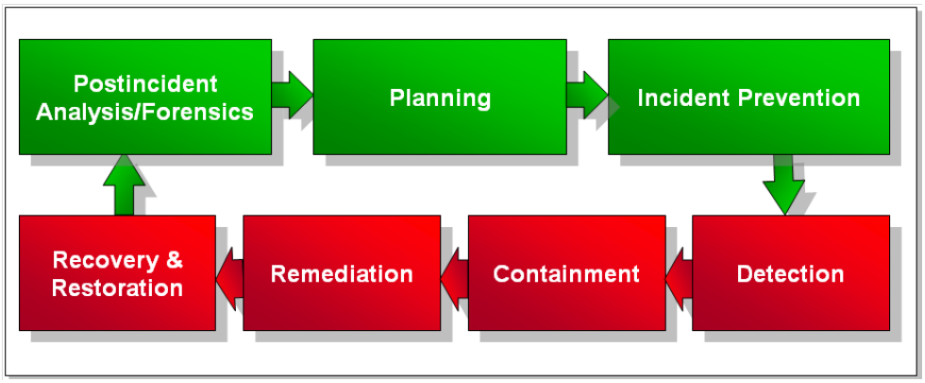
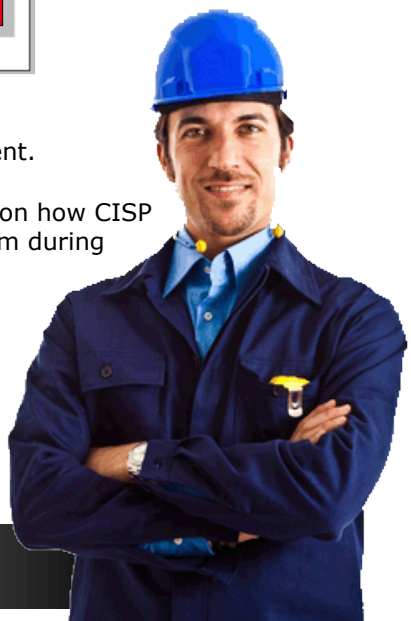


Figure 1 is from an excerpt of the Homeland Security October 2009 Recommended Practice, Developing an Industrial Control Systems Cyber Security Incident Response Capability document.

Future articles will go more into detail in each of the areas identified above and provide details on how CISP can support the effort to put comprehensive Incident Response Plans in place and maintain them during the lifecycle of the Cyber Security Programs.

This months contributor to Consultant's Corner is
Bill Owen
Consultant, Critical Infrastructure & Security Practice
Invensys
bill.owen@invensys.com



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**