The Global Cyber Advisor

by the Cyber Security Services Group

January 2015
Volume 40

Industrial Control System (ICS) Security market worth $8.73 billion by 2019

From www.prnewswire.com, 1/1/2015

The global Industrial Control System (ICS) Security Market is estimated to be $6.18 billion in 2014 and is expected to grow to $8.73 billion in 2019. This represents an estimated Compound Annual Growth Rate (CAGR) of 7.2% from 2014 to 2019. In the current scenario, the power, energy and utilities vertical security continues to be the largest segment, in terms of spending and adoption, for ICS security solutions.

this issue

DST Expands, Adding Cyber Security Solutions

2015 will definitely be a year of change, starting with the transitioning of the Cyber Security Services team to the Schneider Electric Digital Services Transformation (DST) group. Cyber Security Services was established under Invensys in 2006 with a focus on industrial cyber security assessments and solutions. The move to DST will create an even larger opportunity for both Schneider Electric as well as our clients. This newsletter is just one of the ways we communicate to the field about what is new in cyber security. The newsletter is published monthly, going back to October 2011, with back copies available on our website.

2015 also brings changes to the newsletter. Our newsletter content will include:

- **Page 1 Cover Story**: a cover story that addresses relevant industry-related cyber issues
- **Page 2 Cyber Central (New)**: articles focusing on the "who, what, and how" of Cyber Security Services
- **Page 3 Industry News (Updated)**: news stories that directly impact the industrial OT cyber security space around the globe; each headline will now include a tag that references the industry and region for easier reading
- **Page 4 Cyber News**: general cyber security news articles that address the global cyber security landscape
- **Page 5 Consultant's Corner**: each month, one of our consultants addresses a specific technical cyber security topic
- **Page 6 Cyber Security Services**: the last page of the newsletter, which highlights information on our team and our social media contacts for additional information

As we move into the new year, we want to let you know how excited we are on to embark on this new transition and look forward to any way we can work with you to address your cyber security needs.

Cyber Security Services by Schneider Electric

January 2015 / Volume 40

Cyber Central

Cyber Central is a new section in our newsletter that allows us to share who we are, what we do, how we do it, and how we benefit our customers.

Who We Are

Cyber Security Services is a global cyber security team that leverages specialized cyber security knowledge and extensive industry experience in addition to an in-depth network design and implementation background. The Cyber Security Services team is made up of process engineers, network engineers, and IT specialists who have backgrounds in systems security, network design / remediation, data communications, network protocols, and wireless RF. Schneider Electric's Cyber Security Services team represents a cross-section of industries such as oil and gas, power, mining, chemicals, smart platforms, and wastewater, which provides us ability to work alongside clients and communicate effectively with cross-functional teams.

What We Do

Cyber Security Services delivers cyber security solutions that address industries' growing needs for regulatory security compliance as well as corporate mandates and best practice policies, with a focus on Industrial Operation Technology (IOT) space while helping the client bridge the IT space. The solutions that we deliver are platform-agnostic and focus on helping customers with their cyber security compliance requirements. All of our solutions are hardware, software, and product independent.

The cyber security team provides a security methodology that we can deliver. We do not provide a singular hardware or software point solution such as anti-virus software or firewalls like many IT security companies do. On their own, these technologies fall short, missing the security target and providing a false sense of security. You only have to ask yourself a few questions to understand why:

- Who is going to keep my anti-virus software updated and push the anti-virus updates out to the network?
- Who is going to develop my custom firewall rule sets?
- Who is going to keep my firewall up-to-date?
- Who understands the nature of my network?

We believe that the best approach to developing or maintaining a cyber security program is our cyber security methodology. We work closely with clients to help them understand their needs and develop a true risk-based assessment. From that point, holistic solutions can be developed and installed.

Since our approach is methodology-based and not point solution-based, our team is truly able to be platform-agnostic and product independent.

In upcoming months, we will focus in more detail on How We Do it and How We Benefit Our Customers. Next month, we will delve into the cornerstone of our approach, the Cyber Security Lifecycle Methodology.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
January 2015 / Volume 40

Industry News

Oil and gas sector in fear of hackers as cyber attacks surge 179% (Industry/Oil & Gas)
From www.arabianbusiness.com, 12/27/2014

On 15th of August 2012, Saudi Aramco, the largest oil producing company in the world, fell victim to one of the most notorious cyber attacks in the region's history. A self-replicating virus struck as many as 30,000 of Aramco's Windows-based machines causing damage, that took the oil giant as many as two weeks to recover from. More than two years later, the incident is still fresh in the industry's mind, and very rightly so, as the threat of cyber espionage has never been greater. According to a study by PwC, the number of reported cyber attacks carried out on oil and gas companies last year soared above 6,500 cases - a 179 percent increase from the year before. Frost & Sullivan has also reported that cyber security uptake is expected to surge and become "the highest-priority area for oil and gas companies."

Power network under cyber attack sees UK increase defenses (EU/ Power)
From www.bloomberg.com, 1/8/2015

The U.K. government is one step ahead of hackers trying to turn off the country's lights -- for now. The prospect of cyber-attacks on the nation's power network is a major threat to the country's security, according to James Arbuthnot, a member of parliament who chaired the Defense Select Committee until last year. He plans to visit National Grid Plc next month to discuss the issue. "Our National Grid is coming under cyber-attack not just day-by-day but minute-by-minute," Arbuthnot, whose committee scrutinized the country's security policy, told a conference in London last year. "There are, at National Grid, people of very high quality who recognize the risks that these attacks pose, and who are fighting them off," he said, "but we can't expect them to win forever."

Nuclear sector needs overhaul (APAC/Nuclear)
From koreajoongangdaily.joins.com, 1/3/2015

Despite mounting fears over a series of cyberattacks and the leaked blueprints of a reactor at the state-run Korea Hydro and Nuclear Power Corporation (KHNP), nothing has really happened. A self-professed "antinuclear group," which warned it would shut down the corporation's nuclear reactors by paralyzing their operational systems, did not follow through on its threats. And because not a single fatal nuclear accident has occurred, the Korean government and the KHNP are trying to sail through the issue.

Oil and gas industry preparing for cyber attacks (NA/Oil & Gas)
From www.630ched.com, 1/23/2015

As if the dropping price of oil wasn't enough to worry about, now the oil and gas industry is bracing itself for cyber attacks. A conference will be held in Calgary this week that will focus on cyber security for the industry for the first time ever. Producer John O'Connor tells the Alberta Morning News that the attacks on industry can vary. "They go from tier one, state sponsored attacks, to 'hacktivists,' to corporate espionage" he says. "The attack service is pretty wide. We've seen in 2014 that it was kind of the year of the breach, so cyber security is definitely a major issue." The summit will feature a live-hacking demonstration and explanation of common cyber security attacks and how to defend against those. But, O'Connor says an attack on threat intelligence is the main focus.

Hackers could infiltrate NSW traffic and sewage systems (EU/Water)
From theage.com, 1/25/2015

Hackers could infiltrate Sydney's traffic light network and cause accidents or road chaos, an official investigation has found, raising serious doubts over the preparedness of the state's vital infrastructure to ward off cyber attacks. The technology controlling Sydney's water supply and sewers should also be more secure, and the privatization of water treatment hampers checks on cyber security, the probe by NSW Auditor-General Grant Hehir found. He called on government operators of other critical infrastructure to heed the lessons learnt.

Utilities boost focus on cyber security as FERC adopts new standards (NA/Power)
From www.utilitydive.com. 1/20/2015

Cyber security is moving up the ranks of utility industry concerns and now polls fourth, up from sixth, Black & Veatch said in its annual survey of the electric industry's strategic direction. The increased focus follows decisions last year by federal regulators to bulk up physical as well as virtual security of the nation's power grid. While utility spending on security has typically lagged behind reliability and carbon control, new threats and a regulatory focus on grid defense could begin to drive additional investment.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
January 2015 / Volume 40

Cyber News

Sony hack signals 'new normal' in cyber security

From www.nextgov.com, 1/6/2015

The Sony hack copied a multinational company's financial documents, its employees' personally identifiable information and years' worth of embarrassing – and poorly written, it must be said – emails from high-level executives and released them all for the world to see. But for many cybersecurity observers, the real eye opener was how the hack illustrates today's cyber landscape: It's likely to get worse before it gets better. Meanwhile, as Sony's image continues to tarnish with each leaked, scandalous revelation, the company experienced an added layer of suffering other data-breached companies -- Target, Neiman Marcus and Home Depot -- had avoided. "This is the new normal," said Rob Roy, federal chief technology officer for HP Enterprise Security. "I don't think we'll see attacks like this slow down. Defenders are getting better, but attackers are getting more numerous and also getting better."

60% in IT expect a cyber attack on their organization

From pacific.scoop.co.nz, 1/22/2015

A new global survey of more than 3,400 members of IT association ISACA shows that close to half (46 percent) of respondents expect their organization to face a cyber attack in 2015. Locally, in Australia/New Zealand (ANZ), respondents feel that attack is even more likely with 61 percent expecting a cyber attack this year. This is concerning, since less than half of ANZ IT professionals (43 percent) say they are prepared, likely due to a global shortage of skilled cyber security personnel.

Most EU businesses unclear on latest cyber security laws

From www.computerweekly.com, 1/27/2015

Most businesses in the UK, France and Germany feel guidelines to achieve compliance with new European Union cyber security legislation are unclear, a study has revealed. A third of organizations polled also do not understand the impact of the coming cyber security legislation, according to a study by security firm FireEye. The study shows that many organizations in Europe are unprepared for the changes and are challenged by the cost and complexity of complying with new EU data security legislation. Only 39% of organizations polled said they have all the required measures in place for the NIS. Only two-thirds said their organizations fully understand the impact of the NIS and GDPR regulations.

Cyber attacks cost companies $400 billion every year

From fortune.com, 1/23/2015

Last year, the insurance industry took in $2.5 billion in premiums on policies to protect companies from losses resulting from hacks. Lloyd's, the British insurance company, is known for specializing in obscure risks. When civilians finally push off into space, they will likely be insured, along with the aircraft they travel in, by Lloyd's. But one initially rare insurance product has become far more common: hack coverage. Inga Beale, the CEO of Lloyd's, which manages a clearinghouse for insurance policies, said that demand for cyber insurance has grown considerably in recent years. Last year, the insurance industry took in $2.5 billion in premiums on policies to protect companies from losses resulting from hacks. That was up from around $2 billion a year before, and less than $1 billion two years before that.

A cyber attack has caused confirmed physical damage for the second time ever

From www.wired.com, 1/8/2015

Amid all the noise the Sony hack generated over the holidays, a far more troubling cyber attack was largely lost in the chaos. Unless you follow security news closely, you likely missed it. In a German report released just before Christmas (.pdf), hackers struck an unnamed steel mill in Germany. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive"—though unspecified—damage. This is only the second confirmed case in which a wholly digital attack caused physical destruction of equipment. The first case, of course, was Stuxnet, the sophisticated digital weapon the U.S. and Israel launched against control systems in Iran in late 2007 or early 2008 to sabotage centrifuges at a uranium enrichment plant.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
January 2015 / Volume 40

Indicators of Compromise and Effective Incident Handling: Part 2*

*This article is a follow-up to last month's article, which can be found here.

Why is it so critical to organizations to have a detailed and concise incident handling process? As illustrated in the previous article, once an indicator of compromise has been discovered, incident handling (IH) should begin right away. In order to properly isolate the infected machine and begin the investigation process and ultimately remediation, a incident handling program should have already been in place and previously tested. Without this process already in place, a recipe for disaster and ultimately failure will ensue.

The basics for a successful incident handling program can best be described in six phases. This is meant to be a brief outline of the proper structure for the IH process. A common acronym that can be used to identify the six phases of incident handling s PICKERL:

Preparation: The team should be ready and able to handle an incident at a moment's notice. Proper policies should already be instituted giving them prior authorization to conduct business. Plans should already be in place for what to do, who to contact, call trees, etc. Conventional and alternate forms of communication should be established along with the use of qualified and properly trained individuals with all the necessary tools.

Identification: This phase deals with the detection and determination of whether a deviation from prior established standards and baselines has occurred within the organization and warrants an investigation.

Containment: The initial purpose of this phase is to limit the damage to and prevent any further damage to company data and assets. There is also what is considered short-term containment to immediately limit the impact of the incident before more infections occur (such as removing network access to an infected system), but is not intended to be a long-term solution. System backup is also essential to this phase for the purpose of conducting digital forensics to establish the root cause of the issue and may also be required for legal and regulatory reasons as well. Long-term containment is essentially where the affected systems are "patched" with a temporary fix so they can be re-introduced into production until a vendor patch or other permanent solution becomes available, so as not to interrupt the business process.

Eradication: This phase is primarily concerned with the actual removal and restoration of the affected systems. Continued documentation is essential in this phase, as well as all of the phases, so as to answer the questions of Who, When, Why, Where, What and How (especially if there is to be legal action sought against the offending party(ies)). This phase also helps to identify where your network's defenses should be further fortified to prevent future infections.

Recovery: This is the phase where the affected system(s) are formally re-introduced into the production environment and where they are tested, monitored, and validated to show that everything has returned to the normal baseline operating conditions as compared to a known good state.

Lessons Learned: This phase should easily be considered the most important of them all. In this stage, it is critical that all documentation during the incident has been completed, as well as any other documentation that could be beneficial to future incidents. A well-written report should be submitted to the IH team and management for peer review. This report should provide a play-by-play of the entire event from start to finish and it should be able to answer the Who, What, When, Where, Why, and How questions that came up during the investigation. This document can also be used as training/instructional material for new team members as well as thorough review of what went wrong, how it was fixed, and how to prevent future compromises.

As you can see, a successful incident handling team cannot be successful without the proper policies and procedures having already been established and tested. Imagine how much harder it would be to do all of this "on the fly" without a time-tested program, but then imagine how much more successful (and smoother) a team would be with these procedures already in place. At its core, effective incident handling is essentially what makes your cyber security better by learning not only what caused the infection, but also who perpetrated this, why they would want to infiltrate your organization, what they were able to compromise/ steal, where in your systems you are vulnerable, how it happened, and how to better prevent it from ever happening again.

This month's contributor to Consultant's Corner is Paul Pelletier
Consultant, Critical Infrastructure & Security Practice, Invensys
paul.pelletier@invensys.com

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
January 2015 / Issue 40

Cyber Security Services

Schneider Electric's Cyber Security Services organization has the 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 Cyber Security Services include:

Hardware Independence

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

Regulation Knowledge

Cyber Security Services 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 Cyber Security Services 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

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

Proven Methodology

Cyber Security Services follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the lifecycle approach are Assessments, Development, Implementation, and Management.

Schneider Electric

For additional information please visit us at
http://iom.invensys.com/CyberSecurity

1650 West Crosby Road, Carrollton, TX 75006 ▪ P 972.323.1111 ▪ F 888.758.7675 ▪ www.schneider-electric.com