The Global Cyber Advisor

by the Cyber Security Services Group

Schneider Electric

June 2015
Volume 45

this issue

World's nuclear facilities at risk from cyber attacks
From www.hstoday.us, 6/5/2015

The international community must intensify efforts to protect the world's nuclear facilities from cyber attacks, the head of the United Nations nuclear watchdog declared on June 1 as he opened the organization's first-ever conference on the issue at the International Atomic Energy Agency's (IAEA) headquarters in Vienna. Sounding the alarm in front of more than 650 experts from 92 member states, IAEA Director General Yukiya Amano said the inaugural International Conference on Computer Security in a Nuclear World sent "an important message" that the world is finally "serious about protecting nuclear and other radioactive material." "Reports of actual or attempted cyber attacks are now virtually a daily occurrence," Amano affirmed, warning that the nuclear industry had not been immune from the global threat. "Last year alone, there were cases of random malware-based attacks at nuclear power plants and of such facilities being specifically targeted."

Information Technology (IT) vs. Operational Technology (OT)

The world of traditional Information Technology (IT) has morphed greatly over the years into non-traditional roles, such as supporting manufacturing and process control systems. As technology advances, so too must the skill sets, roles, and responsibilities of IT professionals. Companies' heavy reliance on IT and the evolution of skill sets required to support process manufacturing has outpaced the current skill capabilities and range of IT professionals. This evolution has given rise to a new role, Operational Technology (OT). The OT role focuses on the process controls required to operate the manufacturing side of the business. The differences between OT and IT can be somewhat confusing for those on either side when it comes to the specific roles each department plays within a company, but the OT departments and IT departments must work together to develop a company's overall system policies as well as a cyber security compliance program, with both departments responsible for their side of the business.

An effective critical infrastructure cyber security plan requires clearly defined and coordinated roles and responsibilities among OT personnel and IT. However, as critical infrastructure systems and assets become more interconnected, accountability gaps as well as perceived overlaps have formed between the functional roles.

	Information Technology (IT)	**Operational Technology (OT)**
Purpose	Transaction Systems; business systems, information systems, IT security standards	Control Systems; control or monitor physical processes or equipment, regulatory security standards
Architecture	Enterprise wide infrastructure and applications (business)	Event-drive, real-time, embedded hardware and software (industrial)
Interfaces	Operating systems and applications, Unix, GUI, Web browser, terminal, and keyboard	Electromechanical, sensors, Windows, actuators, coded displays – PLC, SCADA, DCS
Ownership	CIO, finance and admin. departments	Engineers, technicians, operators, and managers
Connectivity	Corporate network, Internet, IP-based	Control networks, hard wired twisted pair and IP-based
Role	Supports business applications and office personnel	Support controls processes and plant personal safety

In many industries there has been a shift toward more regulatory compliance and less comprehensive security. The existing federal and state regulatory environment creates a culture within the utility industry of focusing on compliance with cyber security requirements instead of a culture focused on achieving comprehensive and effective cyber security. Cyber security is enhanced when IT and OT converge, but failing to address both the corporate and regulatory cyber security requirements can be detrimental to network security.

Cyber Security Services by Schneider Electric

June 2015 / Volume 45

Cyber Central

How We Benefit Our Customers

Earlier this year in the January newsletter, we introduced ourselves and explained what we do at Schneider Electric. Then in February, we began our four-part "How We Do It" series, outlining our lifecycle methodology: Assess, Develop, Implement, and Manage. Now that we have established who we are, what we do, and how we do it, this month we would like to talk about how we benefit our customers.

Every customer has something they need to protect, regardless of region or industry. The Cyber Security Services team works directly with customers, leveraging our cyber security lifecycle methodology. We have identified seven critical building blocks that provide a foundation every customer will benefit from. These are implemented using the lifecycle methodology.

1. **Identification of Critical Assets**
   What items are essential to everyday operation that need to be protected?

2. **Electronic Access Controls**
   What measures are being taken to block unauthorized access to critical company assets?

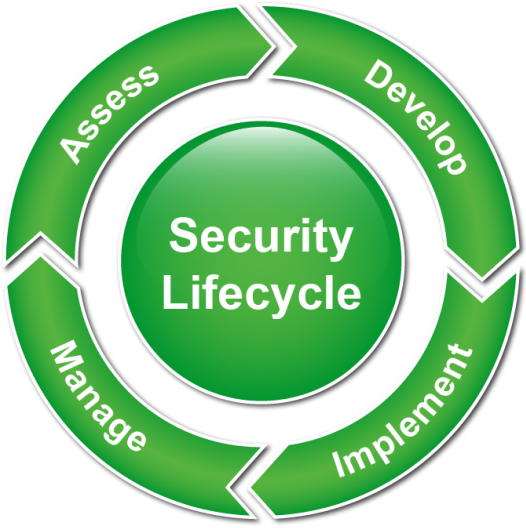
3. **User Access Controls**
   What are user privileges and how are they set to help prevent network interruption?

4. **Patching**
   What applications need regular updating in order to fix possible security vulnerabilities?

5. **Anti-Virus and Device Control**
   What elements are required to prevent malware and malicious cyber events?

6. **Disaster Recovery**
   What program is in place for backup and recovery if disaster strikes?

7. **Logging**
   What procedures are being followed to record and report system events?



Schneider Electric

The Global Cyber Advisor
Cyber Security Services
June 2015 / Volume 45

Industry News

US believes China behind cyber security breach affecting at least 4M federal employees (NA)

From www.foxnews.com, 6/5/2015

Hackers based in China are believed to be behind a massive data breach that could have compromised the personal data of at least 4 million current and former federal employees, U.S. officials said. Sen. Susan Collins, R-Maine, a member of the Senate Intelligence Committee, told the Associated Press that investigators suspect the cyberattack was carried out by the Chinese. She said the breach was "yet another indication of a foreign power probing successfully and focusing on what appears to be data that would identify people with security clearances." If confirmed, the incident would be the second major breach by Beijing in less than a year. A spokesman for the Chinese Embassy in Washington called such accusations "not responsible and counterproductive."

UK firms failing to assess cyber threats, study shows (EU)

From www.computerweekly.com, 6/16/2015

Many UK firms are failing to adequately assess customers and trading partners for cyber risk, a study has revealed. As a result of this failure, businesses are making themselves more vulnerable to cyber attacks, according to the report by insurance broker and risk management firm Marsh, which polled risk managers and chief financial officers from more than 100 large and medium-sized UK firms. The firm's cyber risk survey found nearly 70% of respondents do not assess the suppliers and/or customers they trade with for cyber risk. More than half of respondents also stated their organizations have not been asked to demonstrate a competent standard of their IT security practices to their bank and/or customers to do business with them.

NatGas, oil industry in 'crosshairs' of malicious cyber attacks (EU, APAC, NA)

From www.naturalgasintel.com, 6/8/2015

The threat of cyber attacks is becoming increasingly likely within the energy industry, as organized "threat actors" aggressively attack operations and pilfer data from global businesses, according to a global survey by PwC. In PwC's Global State of Information Survey (GSISS) 2015, analysts said oil and gas companies are in the "crosshairs of malicious cyber adversaries," with well funded operators infecting industrial control systems of thousands of organizations across North America, Asia and Europe. "An attack on a Middle Eastern oil company in 2012 destroyed 30,000 computers and erased a range of significant documents," PwC's report noted. "It was revealed in late 2014 that the 2008 explosion of an oil pipeline in Turkey was caused by hackers, making it one of the first times a cyber attack has successfully been used to destroy critical infrastructure." The attacks to date have not impacted production capabilities but they are becoming "progressively maleficent, sophisticated and difficult to detect," PwC found. Increasingly, cyber criminals target oil and gas companies to lift intellectual property (IP), sabotage websites, harm reputations and disrupt production.

Security experts warn chemical plants are vulnerable to cyber attacks (EU)

From www.rsc.org, 6/10/2015

Security experts are warning that the computers controlling machinery in chemical plants, power stations and other critical infrastructure are vulnerable to attacks from hackers, and that more work is needed to prevent control of critical equipment falling into the wrong hands. Last week, the UK government unveiled the results of a survey that showed the average cost of a serious cybersecurity breach has more than doubled since last year – rising from £600,000 to £1.46 million. And the UK Office of Cyber Security and Information Assurance – the UK government body organising cybersecurity policy – recently estimated that cybercrime costs the UK £27 billion every year. But in the industrial sector – where computer-controlled equipment is commonplace – the threats go beyond financial ruin. 'Virtually all chemical plants have some sort of computer-based automated control system,' says Eric Cosman, who has advised the chemical industry on cybersecurity. 'If you somehow compromise [that system] bad things could happen depending on the nature of the plant – that could range from spills of material, to some sort of overpressure or venting, or in the worst case even some sort of explosion.'

Stuxnet and Shamoon attacks could knock power grids offline (EU)

From www.v3.co.uk, 6/11/2015

Cyber attacks targeting critical infrastructure could take power grids offline, according to Graham Wright, chief information security officer at National Grid. Wright gave the warning during a Westminster eForum session attended by V3 where he said that the threat posed by malware like Stuxnet and Shamoon is real and serious. "[National Grid is] the critical infrastructure, and nothing moves without infrastructure. So we're at the center. If we go down the nation goes down," he said. "This means we're not interested in cyber security for the sake of it. We're interested in it as we care if the lights go off. "We're worrying about stopping threats into the industrial part of what we do. Stuxnet and Shamoon are the things that are important to us, not what happened to Sony or J P Morgan."

The Global Cyber Advisor
Cyber Security Services
June 2015 / Volume 45

Cyber News

State-sponsored cyber attacks are the new normal says Kaspersky Lab

From www.thememo.com, 6/16/2015

Stuxnet, Duqu and Flame might not mean much to most people but they are all examples of state-sponsored cyber attacks which David Emm, a principal security researcher on Kaspersky's global research and analysis team, and his team were pivotal in discovering. State-sponsored cyber attacks first made headlines in 2010 when Stuxnet, a computer worm of alleged Israeli origins destroyed a fifth of Iran's nuclear power plant capabilities. Emm says state-sponsored cyber attacks like Stuxnet are a small but now normal part of the cyber security landscape. Kaspersky classifies around 0.1% of cyber attacks as state-sponsored or state-supported cyber attacks. This compares to 9.9% of cyber attacks which are examples of targeted attacks on organizations and the remaining 90% which are non-targeted viruses or malware. But despite state-sponsored attacks being responsible for such a small number of attacks, Emm says the risks are far higher: "The potential impact of these attacks will always be bigger than the numerical significance of these attacks."

Cyber attacks cost British industry £34bn a year

From www.telegraph.co.uk, 6/10/2015

Defending Britain against cyber attacks and repairing the damage done by hackers who penetrate security systems costs businesses £34bn a year. The huge price tag of dealing with the growing threat of online crime was revealed by research from think-tank CEBR and computer security group Veracode. Just over half – some £18bn – of the total comes from lost revenues as the result of successful attacks, with the remaining £16bn representing companies' increased spending on IT as they beef up their defenses. However, the threat of online attacks is also limiting companies' ability to grow, with seven out of 10 chief technology officers saying that cybersecurity policies "stifle" innovation at their businesses.

British military targeted by thousands of cyber attacks a day

From europe.newsweek.com, 6/26/2015

Britain's Ministry of Defense fends off thousands of cyber attacks every day while its military systems log more than a million suspicious incidents on a daily basis, a security official has told the Financial Times. As more critical infrastructure has become dependent on digital communication, cyber warfare is an increasingly important national security issue. The US defense secretary Ash Carter warned earlier this week, a cyber intrusion in a Nato state's network would be costly and could trigger a collective response that extends beyond cyberspace. Earlier this year former Nato secretary general Anders Fogh Rasmussen claimed cyber security had become part and parcel of collective security and urged allies to heighten their defenses against unconventional warfare. The head of the British armed forces' cyber defense program Brigadier Alan Hill has said that his unit picks up as many as a million suspicious cyber incidents a day on its network, which he says if left unmanaged could lead to a breach, allowing for a cyber attack.

86% energy professionals confident about cyber crime detection within a week

From www.power-technology.com, 6/26/2015

Approximately 86% of energy professionals are confident about detecting cyber attacks on critical systems in less than a week, according to a recent survey by US based software firm Tripware. The study was conducted through Dimensional Research. It polled the opinions of more than 400 executives and IT professionals in the energy, oil, gas and utility industries to assess their views on cyber security and compliance initiatives. Respondents from all the sectors were found to be highly confident about their organizations' capabilities, with 49% claiming that they can detect a cyber attack on critical system within 24 hours. The firms are, however, underestimating the 'sophistication, persistence and evasive technology' of the cyber attackers, she said. As well as highlighting the misplaced trust of the energy security professionals, the survey also indicated that 94% among them agree to being a target for such cyber crimes. While merely 3% said that it would take more than a month to detect an attack on their firm's cyber system, 83% believed that such attacks can physically damage their infrastructure.

Hackers outpacing cyber defense, says ex-FBI official

From www.cbsnews.com, 6/3/2015

The cyber attack against Polish airline LOT is reinforcing concerns that lapses in security are leaving companies at risk. According Shawn Henry, former FBI executive assistant director Shawn Henry, attackers are winning the fight. "The adversaries -- the offense outpaces the defense right now," Henry said. The attack temporarily paralyzed LOT's computers at Warsaw's Frederic Chopin airport, affecting some 1,400 passengers. It also disrupted their ability to schedule new passengers and grounded 11 existing flights.

EU agrees on unified data security laws

From thehill.com, 6/15/2015

European Union member states signed off on a broad restructuring of their data protection laws. The framework is a major step forward in the effort to unify the 28 member countries' data security rules and levy fines against companies that break those rules. The single code is an attempt to better secure people's digital data and fight back against the rising tide of hackers and government-backed spies. "Citizens and businesses deserve modern data protection rules that keep pace with the latest technological changes," said Věra Jourová, commissioner for justice, consumers and gender equality.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
June 2015 / Volume 45

An Effective Patch Management Approach

Why patch systems for vulnerabilities? With every reported virus, malware, or acts of hacktivism, we are reminded that systems have a need for vulnerability patching. Yet, despite the warnings, some companies still do not have a comprehensive patch management process in place to protect their assets.

Don't fret! There is a solution to this problem. Using the best practices step-by-step approach below gives a general idea of the process. However, all systems are slightly different and that's where an experienced cyber security consultant can make the difference. We can help you develop a customized patch management process for your environment.

Step One: Building the plan

First, determine the scope of your network maintenance plan. This will include patches and firmware updates for your workstations, servers, virtual machines, switches, firewalls, and software. Next, define your legal and regulatory requirements. Then decide who will manage the plan and how the plan will be implemented and maintained. Again, all networks are different. Some systems can be set to automatically update real-time while others are patched manually at specified intervals.

Step Two: Taking inventory and analyzing

Create an up-to-date inventory of the systems on the production network. Analyze them to determine their current OS, installed software, firmware version, IP address, missing patches, missing service packs, etc. Network monitoring tools are a big plus in discovering and logging the data for the process.

Step Three: Researching and testing

A study of the identified missing patches and service pack must be completed. A test will need to be done on a non-production asset to verify that the update will not impact the live system or its processes.

Step Four: Remediating

Incrementally apply the patches to bring the systems up-to-date and verify. As a precaution, this step should include a comprehensive backup and roll-back plan as well.

Step Five: Reporting and reviewing

A before and after report will help identify any areas for improvement. Also, documented changes will be needed for audits and proving compliance.

Step Six: Scheduling

Whether it's daily, weekly, monthly, quarterly, or yearly… a proactively scheduled patch management plan will help keep your systems up-to-date.

When networks fail or become compromised due to security breaches, the money, time, and reputation loss can be devastating. Implementing a solution that fits the needs of your network systems, legal requirements, and regulatory requirements can help bolster your company's overall security profile.

This month's contributor to Consultant's Corner is Curt Christian
Consultant, Cyber Security Services
curt.christian@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
June 2015 / Volume 45

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 WordPress!

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://software.invensys.com/services/security-and-compliance-services/cyber-security-services/

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