The Global Cyber Advisor

by the Cyber Security Services Group

Schneider Electric

May 2015
Volume 44

Turkish blackout sparks fears of cyber attack on the West (MENA)

From www.itproportal.com, 5/19/2015

Iran is now believed to be responsible for the blackout that, on 31 March, plunged over 40 million people into darkness in Turkey for over 12 hours, paralyzing the country's principal cities. Intelligence experts are speculating that the attack was a reprisal for support from Turkey to Saudi Arabia in a dispute against the Iran-backed Houthis in Yemen. It could also be related to Turkey's recent moves to topple Syrian dictator Bashar Assad – a strong ally of Iran. Iran-based hacker group Parastoo is already understood to have been actively recruiting hackers with the skills needed to break into the kind of control systems which run power grids and other utilities. The power outage in Turkey represents a significant escalation in the cyber arms race as foreign powers gear up to launch major utilities strikes on cities such as London and New York. Turkey's cyber breach is already providing evidence that Iran now possesses a far more sophisticated cyber warfare capability than it did over two years ago when it is reported to have been responsible for the Saudi Aramco hack, which wiped roughly 2,000 computers and disrupted production for over five days.

this issue

- The Role of Consultants in Cyber Security Services
- Cyber Central
- Industry News
- Cyber News
- Consultant's Corner

The Role of Consultants in Cyber Security Services

In today's market there is no end of third party companies providing cyber security products and services that provide a certain level of security focusing on a specific network elements or product needs. However, customers are still left facing the challenges of integrating a cyber security solution not at the product level but across the plantwide network.

Many third party cyber security services firms claim the ability to provide cyber security solutions. However, the majority fall short because their focus and experience is on the IT corporate enterprise side of security and they lack an understanding of the OT side of the plant as well as working knowledge of digital control systems. Our cyber security services team leverages our cyber security knowledge and OT experience to engage the customer, becoming their thought leader. Only through thought leadership can we engage the customer at the level of intimacy required to provide comprehensive cyber security services. Just like a CPA, what your cyber security consultant knows is as personal as what your accountant knows. Through this relationship, our cyber security consultants help customers to develop their own cyber security program.

Our cyber security services are unique in that we are platform- and system-agnostic and can work with customers at any point in their cyber security program. We work closely with our customers to help them determine where they are today and where they want to be. Through this close relationship, we help the customer develop a plan to realize these goals and objectives. Unlike third party service providers, we nurture and value our customer relationships. By establishing this level of intimacy, we are able to understand all of the customer's network shortcomings and only with this knowledge can we truly develop a comprehensive cyber security program.

Cyber Security Services by Schneider Electric

May 2015 / Volume 44

Cyber Central

How We Do It: Cyber Security Lifecycle Methodology

Part 4 of 4

This month is the final installment of the Cyber Security Lifecycle Methodology. In this month's section, we will review the final stage of the lifecycle: Manage.

Stage 1: Assess
The Cyber Security Services team works with the customer to assess their current network to help identify problems and develop requirements.

Stage 2: Develop
The Cyber Security Services team uses the assessment and the customer's requirements to develop a program unique to their needs.

Stage 3: Implement
The Cyber Security Services team implements the network design from procurement through staging and commissioning of the cyber security solution.

Stage 4: Manage

In many cases, the Implementation stage would be seen as the final step. However, in cyber security, the most important phase is always the management stage. At this stage, we manage the network closely, providing a mechanism to improve and optimize the continuously changing landscape of network usage. Many companies skip or just ignore the management step altogether, believing that their cyber security elements will now protect them going forward. This might be true if the company never makes any changes after the cyber security solution went in; however, this is not practical, as today's process control networks are dynamic. There are always changes, patches, adds, and drops going on.

These daily operational exercises run the risk of compromising the security of the network. Management provides the means to be able to monitor changes, track updates, and detect unconditional behavior alerting you to a potential issue before it can become an event. Stage 4: Management is by far the most important stage to help ensure network integrity.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
May 2015 / Volume 44

Industry News

Executives prepare for potential cyber attacks on energy industry (NA)

From wabe.org, 5/6/2015

The Department of Homeland Security says more than half of all cyber attacks in 2013 targeted the energy industry. On May 5, more than 100 executives and law enforcement officials went through a series of mock cyber attacks at Kennesaw State University's Marietta campus. In the first portrayal: a couple of military veterans buy explosives on eBay. They used the explosives to bomb a fictional water plant in Cobb County. Cyber security professionals and executives have one hour to come up with a response. Utility companies are popular targets. Bryan Ferris is with the Technology Association of Georgia and a former chief information officer with General Electric's energy division, headquartered in Atlanta. He says power outages can be deadly. "If it's a really extended period of time, you start endangering patients, etc." Ferris says. "So it's very critical that we keep power up and available and on the grid."

Utility, security experts warn of mounting threat to grid (NA)

From www.capitalnewyork.com, 5/7/2015

The methods that have been used to attack U.S. power grids have been as rudimentary as firing rifles at substations, and as sophisticated as a computer virus designed to shutter power plants across entire regions. Those physical and cyber vulnerabilities are the Achilles heel of the nation's security apparatus, energy security experts said during the Independent Power Producers of New York's spring conference. "I would say it's the most complex risk landscape since I began at the Department of Homeland Security," said William Flynn, the department's former principal deputy assistant secretary for infrastructure protection. "Not only from acts of terrorism overseas but acts of terrorism domestically."

72% of cyber attacks come from organized crime gangs within UK (EU)

From www.ibtimes.co.uk, 5/12/2015

If we were to believe Hollywood films, hackers have strange accents and live in far-flung countries that you may never have heard of, but new research shows that far and away the majority of criminals carrying out cyber attacks against UK companies are actually based inside the UK. A huge 72% of attacks against businesses in the UK and Ireland are carried out by criminals located on these islands, according to a new report from fraud prevention company ThreatMetrix. This homegrown cybercrime epidemic is not unique to the UK and Ireland, however, with 93% of the attacks taking place in China being carried out from within the country, while France (87%), Germany (81%), Italy (94%) and Russia (85%), also show that hackers look close to home when seeking a victim.

Cyber security is of paramount importance to security of pipeline networks (MENA)

From www.arabnews.com, 5/9/2015

Risk management is of great importance at present for oil and gas operations in the Middle East, and the nexus between this and effective social responsibility planning is increasingly being understood. Recent cyber attacks on Middle Eastern companies systems raised the estimates on the growth of the cyber security industry, because deploying a stronger IT system is very important for the protection of a pipeline. According to a Cyber-Security Expert at ILF, "Cyber security is of paramount importance to the security of oil and gas pipeline networks. A cyber attack against industrial control systems can have a devastating effect on a country's entire Critical National Infrastructure, and yet it is an area which is often given secondary consideration to physical and technical measures. What is required is a systematic and integrated approach to security, and the implementation of an effective, layered, cyber security management system to protect from compromise and manipulation, to detect malicious attempts and, in the event of an attack, to bring about the recovery of the system to a safe and secure state."

Cyber attacks threaten water, wastewater plants EHS activities (NA)

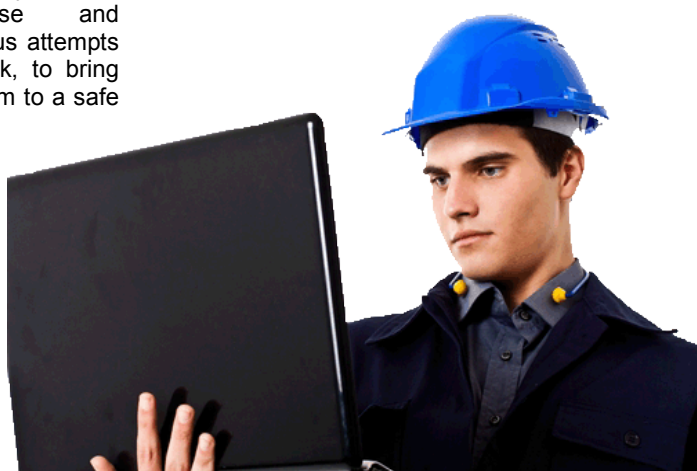
From www.environmentalleader.com, 5/12/2015

Cyber attacks on industrial targets such as water and wastewater treatment plants in 2014 increased more than 25 percent since 2011, according to the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Water & Wastes Digests says according to the report, in 40 percent of those incidents, a lack of detection and monitoring capabilities meant experts did not know how hackers intruded the system.

Cyber attacks targeting oil sector (MENA)

From www.bangkokpost.com, 5/18/2015

A series of cyber attacks has been targeting the oil and gas sector in what appears to be an effective variant of the so-called Nigerian email scam, security researchers said. The scheme dubbed "Phantom Menace" has victimized a number of oil and gas buyers, getting them to pay for non-existent crude, according to a report by Panda Security. According to Panda, the fraudsters offer a large amount of high-quality Bonny light crude oil from Nigeria, which is sought after due to its low sulfur content, "at a very competitive price." The criminals are able to provide fake "documentary evidence that the product exists" and subsequently request the buyers make a deposit of $50,000 to $100,000.



Schneider Electric

The Global Cyber Advisor
Cyber Security Services
May 2015 / Volume 44

Cyber News

Ports, maritime industry at high risk for cyber attacks

From mynorthwest.com, 5/13/2015

The Port of Seattle has far more to worry about these days than just the dispute over Shell's Arctic drilling fleet. A new report finds that the entire maritime industry is woefully unprepared for a cyber attack. A recent study by CyberKeel found that 37 percent of companies running Windows web servers haven't kept up with installing the latest Microsoft security patches. The Copenhagen-based cyber security firm's CEO and co-founder Lars Jensen, said that leaves them vulnerable to hacks.

U.S. asks China to investigate cyber attack targeting U.S. sites

From www.reuters.com, 5/8/2015

The United States said it has asked Beijing to investigate reports that China interfered with Internet content hosted outside the country and used it to attack U.S. websites. "We are concerned by reports that China has used a new cyber capability to interfere with the ability of worldwide Internet users to access content hosted outside of China," State Department spokesman Jeff Rathke said. "The cyber attack manipulated international web traffic intended for one of China's biggest web services companies and turned it into malicious traffic directed at U.S. sites," Rathke told a news briefing. He said the United States asked Chinese authorities to investigate the cyber attack and report its findings. The Chinese government has repeatedly denied it has anything to do with hacking.

Rising cyber attacks costing health system $6 billion annually

From www.chicagobusiness.com, 5/7/2015

A rise in cyber attacks against doctors and hospitals is costing the U.S. health-care system $6 billion a year as organized criminals who once targeted retailers and financial firms increasingly go after medical records, security researchers say. Criminal attacks against health-care providers have more than doubled in the past five years, with the average data breach costing a hospital $2.1 million, according to a study from the Ponemon Institute, a security research and consulting firm. Nearly 90 percent of health-care providers were hit by breaches in the past two years, half of them criminal in nature, the report found. While intrusions like ones exposing millions of consumers at health insurer Anthem Inc. and hospital operator Community Health Systems Inc. have increased risk awareness, most of their peers are still unprepared for sophisticated data attacks, security experts have said.

St. Lucia government moving to strengthen cyber security

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

The St Lucia government says it is moving to strengthen cyber-security in light of the recent attack on the official web site of the St Vincent and the Grenadines government. "This appears to be part of a trend of increasing reports of cyber attacks of various kinds regionally and internationally," according to a government statement. It said "as the Government of St Lucia (GOSL) seeks to continually enhance its online presence and make more of its services accessible online to citizens and other users, it is ever mindful of the increasing importance of cyber security". It said this is why it has embarked on numerous initiatives and taken several proactive measures to reduce the possibility of successful attacks on government information and technology assets as well as to reduce the negative impact should such incidents occur.

Government facing cyber attacks from China, other nations

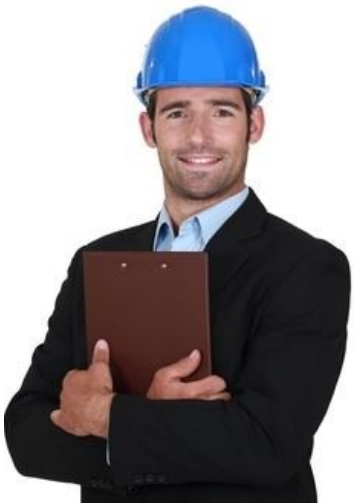
From gagdets.ndtv.com, 5/6/2015

Cyber-attacks are being launched from China and some other nations to penetrate computer networks of government organizations in India, Parliament was informed. To deal with these issues, the government has taken a number of measure to enhance cyber-security and prevent cyber-spying attacks, Minister of Communications and IT Ravi Shankar Prasad said in a written reply to the Lok Sabha. He further said that a crisis management plan has been formulated for countering cyber-attacks and cyber-terrorism. "There have been attempts from time to time to penetrate cyber-networks and systems operating in government organizations. These attacks have been observed to be directed from the cyberspace of a number of countries, including China," the Minister said.

Cyber insurance market booming on rising cyber attacks

From businessdayonline.com, 5/5/2015

As organizations in Nigeria become more reliant on data and more of their businesses conducted over digital channels, there is an increasing need to protect that data and those channels from cyber-attacks – creating a massive opportunity for the cyber insurance market. The cyber insurance market is booming due to rising cyber-attacks, but insurance organizations will need to become much more sophisticated in their approach to assessing and managing cyber risk if they hope to turn cyber policies into a strong and sustainable line of business. The Cyber insurance is among the fastest-growing niches in the industry today. According to recent studies by KPMG, one of the largest professional services companies in the world, "Companies are increasingly seeking cyber breach insurance products that cover the management and costs of notification processes". As fledgling digital economies take off in Kenya, South Africa, and Nigeria, local cybercriminals have emerged and are organizing themselves to take advantage of regional financial services including the nascent and highly popular mobile money industry.



Schneider Electric

The Global Cyber Advisor
Cyber Security Services
May 2015 / Volume 44

Are you more secure today than you were yesterday?

The practice of information security is one of those activities where nothing really bad happens on any given day. Suddenly, one day, data vanishes, unauthorized access is detected, or malware unleashes chaos throughout the network. When things are running as expected, your coworkers and customers notice nothing. But when things go bad, everybody notices and you start receiving those calls from senior management or customers. Due to the dynamic nature of these two opposing forces in information security, silence vs. service disruptions, a few questions need to be answered. How secure are you and are you more secure today than you were yesterday? How do you know if your security measures you implemented are cutting it? These concerns can easily be answered if you are implementing security metrics as part of your information security program. They are vital in the success of any information security program.

Why are metrics so important? They provide visibility into how an information security program is running, educate and provide a common language that can be understood by all parties participating throughout the organization, and enable improvement and optimization of any given process within the lifecycle of the program. Information security metrics are tools that help in determining accountability and promote decision-making through the collection, examination, and reporting of pertinent performance data. Good information security metrics are quantifiable in nature, objective, based on a formal model, universally acceptable, inexpensive, automated, obtainable, and most importantly repeatable. The most common metric types in use are: process security metrics, network security metrics, software security metrics, and people security metrics.

Information security metrics fall into two basic categories: quantitative and qualitative. Quantitative metrics take data that can be broken down into hard numbers and easily be measured. Qualitative metrics are measures that reflect reasoned estimates of security by an evaluator of an agreed upon norm, i.e. tests and surveys. The metric development process consists of two major activities: 1) Identification and definition of the current information security program, and 2) selection of specific metrics to measure the application, effectiveness, and impact of the security controls. Before the process starts, an assessment of how much risk an organization handles should be determined. This calculated risk tolerance will help define the goals, outcome, and approach that are appropriate for their security needs and establish which metrics to use. Some industries are very risk adverse and have regulatory authorities that they are beholden to in maintaining compliance with the governing regulations or information security framework to maintain in order to keep their licenses of operation.

Now that you identified what metrics you want to use, a baseline needs to be set. You must establish the normal operating level for each of your metrics in order to determine when something is abnormal. This baseline allows you to establish a trend that should be analyzed to see if it is acceptable to the goals-outcomes defined in your information security program. Once the trend has been established, the security program is in effect. The metrics can now be used to measure the trend for gaps and whether they are increasing or decreasing. Remediation can now be applied toward the discovered gaps by reviewing the existing security controls. If those in place are not sufficient enough, new ones will have to be deployed to replace processes that are ineffective. Anything new that you have to purchase will probably be a tough sell to management. But now, you will now have the metric data to build a compelling report to justify your needs and how critical they are in fulfilling the company's overall business objective.

Metrics need to be a mandatory part of your information security program. Incorporating them into your program is the only way to assess the effectiveness of your security and provide a means to improve any gaps discovered. Since information security is a moving target, it needs to be continuously evaluated and adjusted. New attack vectors, new employees, new equipment, and new processes are just a few examples that will bring change to your program. It will never be a "set it and forget it" type of activity.

This month's contributor to Consultant's Corner is Todd Wheeler
Consultant, Cyber Security Services
todd.wheeler@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
May 2015 / Volume 44

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