The Global Cyber Advisor

by the **Cyber Security Services Group**

Schneider Electric

April 2015
Volume 43

National power grids hit by cyber terrorist onslaught (NA)

From www.itproportal.com, 4/7/2015

An analysis of federal energy records has revealed that parts of the US power grid are attacked online or in person every few days. This threat is now also looming over major cities outside the US such as London. After analyzing federal data and surveying more than 50 electric utilities, USA Today described the power grid as vulnerable to a major outage that could affect millions. Although a cyberattack has not yet caused a major loss of power, the mechanisms guarding the grid undergo small hacks multiple times a week. The Department of Homeland Security was alerted to 151 energy-related "cyber incidents" in 2013, up from 111 in 2012. But, since 2013, the attacks have escalated hugely with probes now continuously taking place, according to the Edison Electric Institute.

this issue

- Information Technology (IT) v. Operational Technology (OT)
- Cyber Central
- Industry News
- Cyber News
- Consultant's Corner

Information Technology (IT) v. 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 personnel. 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	Supports controls processes and plant personnel safety

In many industries, focus has shifted to more regulatory compliance rather than 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, and failing to address both the corporate and regulatory cyber security requirements can be detrimental to network security.

Cyber Security Services
by Schneider Electric

April 2015 / Volume 43

Cyber Central

How We Do It: Cyber Security Lifecycle Methodology

Part 3 of 4

Last month we discussed Stage 2 of our lifecycle methodology, Development, and how it tied back to Stage 1, the Assessment.

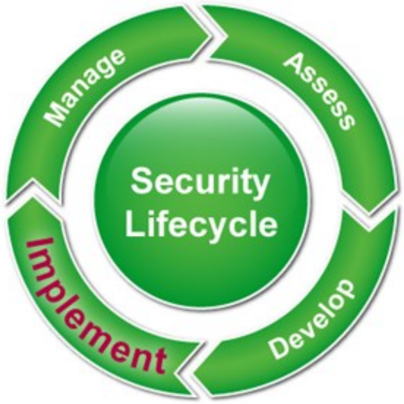
Stage 1: Assess
The Cyber Security Services team works with the customer to assess their current network to help identify problems and develop requirements.

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

This month we will review Stage 3, the Implementation.

Stage 3: Implement

With the Assessment and Development stages complete, the next stage is implementation. At this point, Cyber Security consultants implement the network design from procurement through staging and commissioning of the cyber security solution. This is a very unique point for the Cyber Security Services team. Unlike many Cyber Security consultants that will come in and do a report or assist on a network design, our Cyber Security Services team will actually perform the cyber security solution implementation and cut over. The Cyber Security Services team has not only cyber security knowledge but the industry and control expertise to be able to work seamlessly onsite, interfacing with both the process team as well as the IT team as needed.



Upon completion of the installation, the Cyber Security Services team provides a full set of documentation for the site-specific solution that was just delivered.

Next month in part 4, the final installment of "How We Do It: Cyber Security Lifecycle Methodology," we will review Stage 4, Management.

Industry News

Iran poses growing cyber threat to US (MENA)

From www.yourmiddleeast.com, 4/17/2015

Iran's far-reaching hacking efforts indicate the regime is searching for vulnerable infrastructure that could be hit in future cyber assaults, said the study by private cyber security company Norse and the American Enterprise Institute think tank. "Iran is emerging as a significant cyber threat to the US and its allies," the study said. Iran's skill in the cyber realm has markedly improved in recent years and "Iran has already penetrated well-defended networks in the US and Saudi Arabia and seized and destroyed sensitive data," it said. The hacking, including espionage and attacks, has expanded despite economic sanctions and high-stakes negotiations between Iran and world powers on Tehran's nuclear program, it said.

Hackers have 'begun targeting nuclear power plants,' cyber warfare expert warns (NA)

From www.jpost.com, 4/16/2015

Computer hackers have begun targeting electric and nuclear power plants around the world, as well as other critical infrastructure sites in increasingly audacious attacks, a senior Israeli cyber security expert warned. Col. (res.) Dr. Gabi Siboni, director of the Cyber Security Program at the Institute for National Security Studies in Tel Aviv, said the recent “major infiltration of Sony Pictures and news that Home Depot and Target were victims of cyber-attacks affecting millions of customers is the least of the world’s worries. “The disruption and possible infiltration of critical infrastructure is the most severe form of cyber-attack. Such attacks on airplanes or air traffic control towers, for instance, means that hackers could cause accidents, or even paralyze entire flight systems. As of now, this area of capabilities is the exclusive domain of developed states,” he continued. “I strongly believe, however, that the next 9/11 will happen without suicide bombers aboard the plane with box-cutters, but will occur because of a cyber incident perpetrated by a terror organization,” he said.

Oil and gas platforms at risk of cyber attack (MENA)

From www.khaleejtimes.com, 4/26/2015

Oil, gas and industrial platforms across the Middle East are vulnerable to potentially disastrous cyber attacks, according to a security expert from defence giant Lockheed Martin. Andrew Wadsworth, head of Lockheed Martin’s Process Control Security and a former geologist with over 30 years experience in the oil and gas industry, said that unlike traditional hacking attacks, a cyber assault on an industrial or energy platform has the potential to cause significant real-world damage. “The big difference between securing an industrial control system versus information security is that if an industrial control system goes wrong, it has the potential to create an environmental impact, as well,” he said.

IoT drives Asia-Pacific cyber security to $22B by 2020 (APAC)

From www.enterprisetech.com, 4/8/2015

Spurred by private sector awareness, political turmoil, and cybercrime, Asia-Pacific organizations will spend $22 billion on critical infrastructure technologies by 2020, ABI Research estimates. Spending is expected to increase 17.7 percent between 2014 and 2015, the strongest growth rate globally compared to all other regions, London-based Michela Menting, Digital Security Practice director at ABI Research, told Enterprise Technology. Organizations are buying a mix of off-the-shelf malware and all-purpose anti-spam software, as well as customized solutions designed to help thwart localized, precise attacks launched against specific companies, groups, or individuals, she said.

The West could be crippled by cyber attack on oil refineries, power plants and electric grids, warns former NSA chief (NA)

From www.dailymail.co.uk, 4//2015

The U.S. and her allies are at an ever growing risk of a systemic cyber-assault, with energy infrastructure likely to be hacker's prime target. The stark warning comes from General Keith Alexander, the retired four-star general and former chief of the National Security Agency. 'The greatest risk is a catastrophic attack on the energy infrastructure. We are not prepared for that,' he warned. He envisioned a worst case-scenario where hackers targeted oil refineries, power stations, and the electric grid. The payments nexus of the major banks could also be paralyzed he warned. 'We need something like an integrated air-defense system for the whole energy sector,' he said. Alexander listed five countries able to conduct cyber-warfare at the highest level: the US, UK, Israel, Russia and Iran.

House passes cyber security bill after companies fall victim to data breaches (NA)

From www.nytimes.com, 4/22/2015

Responding to a series of computer security breaches in government and the private sector, the House passed an expansive measure that would push companies to share access to their computer networks and records with federal investigators. The bill, which came after years of false starts and bitter disappointment for the Obama administration, is similar to a measure approved by the Senate Intelligence Committee and headed for that chamber’s floor this spring. The House measure, already largely embraced by the White House, passed, 307 to 116. Should the House and Senate come together on final legislation, it would be the federal government’s most aggressive response yet to a spate of computer attacks that helped sink a major motion picture release by Sony Pictures Entertainment, exposed the credit card numbers of tens of thousands of customers of Target stores and compromised the personal records of millions of people who did business with the health insurer Anthem.

Cyber News

Cyber security gets better, but more needs to be done

From www.arabnews.com, 4/21/2015

Slowly but steadily, Saudi Arabia is becoming less vulnerable to cyber attacks as compared to a couple of years ago, but figures show that a lot still needs be done. Among the vulnerable countries in the world for overall cyber security, the Kingdom was at the 36th position in 2013, but it climbed down to the 42nd position in the following year, that is 2014. This shift indicates a lower number of source-based security threats, including malicious code and spam. Eyas Hawari, Symantec’s country manager for Saudi Arabia, told Arab News that the Internet security threat report shows a tactical shift by cyber attackers. They are infiltrating into networks and evading detection by hijacking the infrastructure of major corporations and using it against them, he said.

Russian hackers got Obama's schedule in White House cyber attack

From thehill.com, 4/7/2015

Russian hackers who hit the White House infiltrated an unclassified computer system and apparently accessed details about President Obama's schedule. While the White House previously sought to downplay the seriousness of the hack, which took place last year, the intruders were able to see information about the president that was not publicly available, CNN reported. Officials briefed on the investigation told CNN that the incident was connected to a Russian cyberattack that also breached the State Department's network. The breach of Obama’s schedule is notable because the White House maintains tight control over information about the president’s activities.

Researchers test brain activity to identify cyber security threats

From phys.org, 4/22/2015

The old adage that a chain is only as strong as its weakest link certainly applies to the risk organizations face in defending against cybersecurity threats. Employees pose a danger that can be just as damaging as a hacker. Iowa State University researchers are working to better understand these internal threats by getting inside the minds of employees who put their company at risk. To do that, they measured brain activity to identify what might motivate an employee to violate company policy and sell or trade sensitive information. The study found that self-control is a significant factor. Researchers defined a security violation as any unauthorized access to confidential data, which could include copying, transferring or selling that information to a third party for personal gains. In the study, published in the Journal of Management Information Systems, Qing Hu, Union Pacific Professor in Information Systems, and his colleagues found that people with low self-control spent less time considering the consequences of major security violations.

Cyber spies hacked Israeli army networks, security researchers say

From www.haaretz.com, 4/17/2015

Hackers have managed to penetrate computer networks associated with the Israeli military in an espionage campaign that skillfully packages existing attack software with trick emails, according to private security researchers. The Israel Defense Forces said it had no knowledge of the alleged hacking. According to the researchers, the 4-month-old effort, most likely by Arabic-speaking programmers, shows how the Middle East continues to be a hotbed for cyber espionage and how widely the ability to carry off such an attack has spread.

FAA hit by cyberattack, finds no damage

From www.usatoday.com, 4/7/2015

The Federal Aviation Administration discovered malicious software from email in its computer system in early February, but the agency said it found no damage from the cyberattack. "The agency immediately took steps to block and contain the virus and clean any affected computers," the FAA said in a statement. "After a thorough review, the FAA did not identify any damage to agency systems."

Taiwan third most targeted country by cyber attacks in Asia

From www.wantchinatimes.com, 4/3/2015

Taiwanese enterprises have come under mounting threat of targeted attacks on their computer networks, a US network security company said Thursday, citing 2014 data placing Taiwan in third place, behind South Korea and Hong Kong, on the volume of advanced persistent threat (APT) activities in the Asia-Pacific region.

User mistakes aid most cyber attacks, Verizon and Symantec studies show

From www.reuters.com, 4/14/2015

When a cyber security breach hits the news, those most closely involved often have incentive to play up the sophistication of the attack. If hackers are portrayed as well-funded geniuses, victims look less vulnerable, security firms can flog their products and services, and government officials can push for tougher regulation or seek more money for cyber defenses. But two deeply researched reports being released this week underscore the less-heralded truth: the vast majority of hacking attacks are successful because employees click on links in tainted emails, companies fail to apply available patches to known software flaws, or technicians do not configure systems properly.

Information Assurance Resource Center: DIACAP to DIARMF

This month's Consultant's Corner features guest author Jesse Wiegand from the Building and Management services team.

Schneider Electric Information Assurance Footprint

Information Assurance Resource Center

Schneider Electric has created the Information Assurance Resource Center (IARC) to spearhead product compliance focused on federal government installations. The IARC team provides Information Assurance Certification and Accreditation activities in support of Schneider Electric contracts. The IARC is comprised of current and prior US Government Information Assurance personnel who are well versed in Information Assurance compliance activities and are responsible for Certification and Accreditation of over 50 systems with 100% success rate, achieving Approval to Operate (ATO) and Certificate of Networthiness (CoN) status. Our professional staff maintains CISSP and Security+ certifications and our analysts are experienced with applicable statutes including the Federal Information Security Management Act (FISMA) and the Computer Security Act (CSA). Our security analysts are often called upon to support IT security policy and implementation in compliance with technical standards from government agencies.

DIACAP to DIARMF

The Department of Defense (DoD) is transforming Information Assurance (IA) policies and practices to align with federal government risk management policies and practices. Under the DoD Information Assurance Certification and Accreditation Process (DIACAP), there were multiple aspects of Information Assurance The DoD was focused on DIACAP and the Intelligence Community used Director Central Intelligence Directive (DCID), while other federal agencies followed National Institute of Standards and Technology (NIST) standards. Early in 2011, a Joint Task Force Transformation Initiative was created with the purpose of having all branches of federal government on the same IA playing field. The outcome–the DoD aligned IA and risk management, policies, procedures, and guidance under the DoD Information Assurance Risk Management Framework (DIARMF). DIARMF is a unified information security framework for the federal government.

The Dilemma

Our Program Manager/Project Manager's primary responsibility is to oversee the development and maintenance of a system that fulfills its stated mission. However, in order for the system to be put into operation, it must receive authorization to operate (accreditation). Therefore, our Manager must ensure the appropriate risk management activities are integrated into the system lifecycle. Usually there is a support contractor in place to provide system development and integration services, but additional Information Security support is needed to oversee risk management activities.

In response to this need, the IARC is pleased to offer information security services to federal Program/Project Managers.

The Next Step

If you have a project with the federal government, chances are you need to comply with federal IA requirements. The IARC is pleased to announce we are fully capable, qualified, and standing by to assist you with all your federal government IA needs. Please don't hesitate to contact us.

This month's contributor to Consultant's Corner is Jesse Wiegand
Information Assurance Program Manager
jesse.wiegand@schneider-electric.com

The Global Cyber Advisor
Cyber Security Services
April 2015 / Volume 43

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.

For additional information please visit us at http://software.invensys.com/services/security-and-compliance-services/cyber-security-services/