The Global Cyber Advisor

by the Cyber Security Services Group

Schneider Electric

October 2015
Volume 49

After fending off cyber attack, FirstEnergy says government coordination lacking (NA)

From www.utilitydive.com, 10/23/2015

Hackers attempted a denial-of-service attack on FirstEnergy's servers this week, but while information on the unsuccessful attempt was quickly shared with the industry and the U.S. government, company officials say there was no response from federal officials, EnergyWire reports. FirstEnergy CIO Bennett Gaines told a House subcommittee this week that information sharing between industry and the government is essential to grid security, but he never heard back from federal officials after reporting the attack. Cyber vulnerabilities are an increasing concern for the industry, amid increased attacks, known vulnerabilities, and estimates that a widespread outage could cause catastrophic damage to the United States' economy.

this issue

What is Cyber Security?

National Cyber Security Awareness Month, celebrated every October, was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online (www.staysafeonline.org). This year marks the 12th year of National Cyber Security Awareness Month, and the subject of cyber security has continued to become more rampant in the news and among consumers and businesses.

But what is cyber security? If you ask 100 people, you may be surprised to find that you get 100 different answers. Cyber security has different meanings to everyone; understandably, it depends on the industry you're in, the process control network you run, and the types of regulations that oversee your specific industry. A control system engineer has a distinct definition, but IT experts may have a completely different definition. To add to the confusion, everybody wants to be cyber secure or they have a mandate to be cyber secure, but because their views are all different, it slows down the process to engage in an effective cyber security program.

Regardless of what definition is the most correct, Schneider Electric focuses on clients' needs and what clients believe cyber security means, since there may be a gap between their definition and their specific needs to comply with best practices, corporate policies, and government regulations. It is also important to understand that cyber security is not just a hardware and software solution but rather how these items are implemented and maintained in a comprehensive cyber security program.

The reasons for implementing cyber security can be almost as numerous as there are definitions for the term itself, yet some will insist they have nothing to protect. Many people understand the need for cyber security, but how do we explain to management why we need it? Consider the questions below:

- Are there competitors who would benefit from your intellectual property?
- Are you sure none of your critical systems "touch" the internet?
- Do you rigorously scan all USB drives and ensure they are under constant surveillance while being used on the plant premises?

A comprehensive cyber security solution is based on an assessment of the current network, development of the cyber security solutions that address the client's needs (regulatory or internal), the implementation of the cyber security solution, and most importantly the management of the solution once it's up and running.

At Schneider Electric, cyber security is viewed as a holistic approach. The bottom line is everyone has something they need to protect. Whatever your definition of cyber security is, the Cyber Security Services team can provide you with a comprehensive solution to address your cyber security needs.

Cyber Security Services by Schneider Electric

October 2015 / Volume 49

Cyber Central

NIST Framework for Improving Critical Infrastructure Cyber Security

Last month, we began a three-part series about the NIST Framework, beginning with the Framework Core. The Core identifies the key activities needed to ensure cyber security and is composed of four elements: Functions, Categories, Subcategories, and Informative References. The Framework provides discussion and examples for these activities, including helpful tables and a cataloging system that assigns the following unique identifiers to the different elements: Identify, Protect, Detect, Respond, and Recover. For this month's article, we will discuss the Framework Implementation Tiers.

The Framework Implementation Tiers

The Tiers describe the increasing degree of rigor and sophistication in cyber risk management practices. They range from Partial (Tier 1), where an organization's risk management practices are not formalized and where risk is managed on an ad hoc and often reactive basis, to Adaptive (Tier 4), where the organization has a comprehensive and organization-wide cyber security program that can be adapted, based on lessons learned and predictive indicators, and where the organization actively shares information with partners.[2]

The Framework acknowledges that selecting the right Tier involves considering the organization's current risk management practices, the threat environment, legal and regulatory requirements, business and mission objectives, and organizational constraints. Although organizations identified as Partial (Tier 1) "are encouraged to consider moving toward Tier 2 or greater," the Framework recognizes that some organizations cannot or need not reach Tier 4, stating that "progression to higher Tiers is encouraged when such a change would reduce cyber security risks and be cost effective."[2]

Tier 1: Partial

- Risk Management Process – Organizational cyber security risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cyber security activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Integrated Risk Management Program – There is limited awareness of cyber security risk at the organizational level and an organization-wide approach to managing cyber security risk has not been established. The organization implements cyber security risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cyber security information to be shared within the organization.
- External Participation – An organization may not have the processes in place to participate in coordination or collaboration with other entities.

Tier 2: Risk Informed

- Risk Management Process – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cyber security activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Integrated Risk Management Program – There is an awareness of cyber security risk at the organizational level but an organization-wide approach to managing cyber security risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cyber security duties. Cyber security information is shared within the organization on an informal basis.
- External Participation – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.[2]

Tier 3: Repeatable

- Risk Management Process – The organization's risk management practices are formally approved and expressed as policy. Organizational cyber security practices are

Schneider Electric

regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.

- Integrated Risk Management Program – There is an organization-wide approach to manage cyber security risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
- External Participation – The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

Tier 4: Adaptive

- Risk Management Process – The organization adapts its cyber security practices based on lessons learned and predictive indicators derived from previous and current cyber security activities. Through a process of continuous improvement incorporating advanced cyber security technologies and practices, the organization actively adapts to a changing cyber security landscape and responds to evolving and sophisticated threats in a timely manner.
- Integrated Risk Management Program – There is an organization-wide approach to managing cyber security risk that uses risk-informed policies, processes, and procedures to address potential cyber security events. Cyber security risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- External Participation – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cyber security before a cyber security event occurs.

Next month we will discuss the Framework Profile, which involves aligning the functions and related activities described in the Core with an organization's specific business requirements, risk tolerance, and resources to establish a roadmap for reducing cyber risk.

References

[1] ICS-CERT ICS-CERT Monitor Oct/Nov/Dec 2013

[2] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

The Global Cyber Advisor
Cyber Security Services
October 2015 / Volume 49

Industry News

Nuclear power plants around the world unprepared for cyber attacks, warns new report (EU)
From www.ibtimes.com, 10/5/2015

Nuclear power plants across the world are getting increasingly vulnerable to cyber attacks as they increase their reliance on digital systems and "off-the-shelf" software, Chatham House -- a London-based nonprofit -- warned, in a new report. Moreover, because of an "element of denial," several nuclear facilities have failed to put in place mechanisms to protect themselves against digital attacks. In addition, even as vulnerability of nuclear power plants increases -- partly because of their outdated control systems -- hacking is becoming even easier to conduct with the availability of automatic cyberattack packages that can be purchased online.

Nuclear power plants at huge risk of cyber attack, study says (EU)
From www.techtimes.com, 10/7/2015

Breaking into a nuclear power plant's computer system may actually be easier than physically breaking into the power plant itself. While nuclear power plants have established physical safety and security measures, many of them still lack the same level of security against cyber attacks, especially when employees still use default passwords like "1234" for computer systems that control a power plant's processes. Based on findings from an 18-month study by UK thinktank Chatham House, the researchers concluded that nuclear facilities will have to ante up against potential cyber attacks as these infrastructures "become increasingly reliant on digital systems and make increasing use of commercial 'off-the-shelf' software, which offers considerable cost savings but increases vulnerability to hacking attacks."

The 5 US industries most uninsured against cyber risk (NA)
From www.ibamag.com, 10/12/2015

The cyber insurance market is a seemingly unstoppable juggernaut. With more than half of US businesses now carrying some form of cyber coverage and the market itself expected to triple in size to $7.5 billion by 2020, it seems the product is just about selling itself. Yet take-up rates for cyber insurance are not spread equally. According to a recent report from Marsh Risk Management Research, while all major industries increased their purchase of coverage in 2014, five markets still trail significantly behind—with the manufacturing industry the most uninsured against cyber risk. Just 8% of companies in this sector purchased standalone cyber insurance last year.

Czechs prepare for cyber attack on nuke plant (MENA)
From www.praguepost.com, 10/7/2015

An exercise simulating a cyber attack on a nuclear power plant and checking Czech experts' readiness to cope with it was held in the new Cyber Polygon of Brno's Masaryk University earlier this month. It is the first exercise of its kind in the Czech Republic. The teams of fictitious attackers and defenders are comprised of IT and cyber experts from academic institutions, ministries, industry and the National Security Office, many of whom really face hackers' attacks in their everyday work. The exercise is to help experts train tackling cyber incidents as a team, Radim Ošťádal, from the National Cyber Safety Center, told journalists. The attacks will continue for several hours, their methods will vary and they will escalate. They may even paralyze the fictitious power plant's operation. The exercise started on Tuesday, when the participants got acquainted with the infrastructure in question and prepared it for hackers' attacks.

Education, energy and finance top UK cyber attack targets (EU)
From www.computerweekly.com, 10/1/2015

More than two-thirds of all advanced cyber attacks in the UK are targeted at the education, energy and financial services sectors, according to a report by security firm FireEye. The Advanced threat report for the first half of 2015 in the Europe, Middle East and Africa region also highlighted an increase in advanced attacks against UK enterprises. After education, energy and financial services, the most targeted industry sectors in the UK were revealed to be aerospace and defense, high-tech, telecoms, entertainment and media, local and state government, and manufacturing.

ISIS is attacking the U.S. energy grid and failing (NA)
From money.cnn.com, 10/15/2015

The Islamic State is trying to hack American electrical power companies -- but they are terrible at it. U.S. law enforcement officials revealed the hack attempts at a conference of American energy firms who were meeting about national security concerns. "ISIL is beginning to perpetrate cyberattacks," Caitlin Durkovich, assistant secretary for infrastructure protection at the Department of Homeland Security, told company executives. Investigators would not reveal any details to CNNMoney -- or cite evidence of specific incidents. But they did say the attacks by the Islamic State have been unsuccessful. Terrorists are not currently using the most sophisticated hacking tools to break into computer systems and turn off or blow up machines.

The Global Cyber Advisor
Cyber Security Services
October 2015 / Volume 49

Cyber News

European organizations 'underestimate cybersecurity risks'

From www.welivesecurity.com, 10/12/2015

Enterprises across Europe need to work harder to better understand and respond to cybersecurity risks, according to a new study from Marsh. The European 2015 Cyber Risk Survey reported that 79 percent of businesses have "a basic understanding of their cyber risk profiles", leaving them extremely vulnerable to cybercriminals. Moreover, the fact that 25 percent of respondents believe cybercrime is not "material enough" to be considered as part of a risk strategy is a significant concern, the authors of the paper commented.

Cyber security attacks costing more than £1.7million, with oil and gas firms at risk

From www.energyvoice.com, 10/8/2015

Almost 10% of companies in the UK are unaware they have been victim to cyber security attacks with incidents now costing an average of £1.7million, according to a new report. The annual survey, which involved more than 10,000 executive from more than 127 countries, showed an escalation in the frequency, severity and impact of cyber -attacks. Insiders – either current or former employers – top the list as a major source of incidents with 14% of companies unsure of how they happened.

US, S. Korea united against cyber and nuclear threats

From www.straitstimes.com, 10/18/2015

United States President Barack Obama and South Korean President Park Geun Hye presented a united front against international cyber threats and the North Korean nuclear threat as the two countries reaffirmed ties, dismissing speculation of cracks in the relationship due to South Korea's overtures to China. Speaking at a joint press conference at the White House, Mr. Obama said "the alliance is on firmer footing than it has ever been", calling it a "linchpin of peace and security" on the Korean Peninsula and across the region. Ms. Park added that the two sides would "open new frontiers of cooperation" in health security, cyber security, and space exploration.

Cyber security firm says Chinese hackers keep attacking U.S. companies

From www.nytimes.com, 10/19/2015

With President Xi Jinping of China beside him at a news conference in the White House Rose Garden last month, President Obama said the two had come to an agreement that China and the United States would refrain from attacks aimed at pilfering company intellectual property or trade secrets for commercial advantage. Less than a day after that announcement and after Mr. Xi had met in Seattle with the executives of leading American technology companies, a hacking group accused of having links to the Chinese government attacked one such company, looking for trade secrets. The attacks continued in the three weeks since Washington and Beijing signed the security agreement.

Australia number one for cyber security breaches

From www.accountantsdaily.com.au, 10/22/2015

Incidences of cyber security breaches within Australia were the highest worldwide over the past 12 months, representing an increase of 109 percent. According to local data from PwC's The Global State of Information Security Survey 2016, the dramatic increase dwarfed a comparative 38.5 percent increase in cyber-security threats globally. "The frequency of cyber security incidents in Australia almost tripled that of the rest of the world from 2014 to 2015," said Steve Ingram, PwC Australia and Asia-Pacific cyber leader, commenting on the figures which revealed Australia incurred 9,434 separate incidents involving cyber security.

Study shows cyber-crime average costs are £4.1m per year in the UK

From www.scmagazineuk.com, 10/13/2015

In the HP Enterprise Security sponsored "2015 Cost of Cyber Crime Study: UK", the Ponemon Institute conducted 326 interviews with personnel from 39 UK companies to assess the incidence and cost of cyber -crime for businesses. The number of cyber-attacks in the UK continues to grow in frequency and severity. Some of the key findings of the study include average cost of cyber-crime by an organization's size and industry, type of attack influences cost of cyber-crime and cost components. The average cost of cyber-crime is £4.1 million per year. This is a 14 percent increase in the average cost from last year.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
October 2015 / Volume 49

New Credit Card Use Methods

While this article does not specifically address critical infrastructure or industrial cyber security, you may have read recently about many instances of credit card data being stolen from retailers. What has been the major security shortcoming allowing this credit card data to be stolen? It has been a lack of encryption.

Credit cards in use in the United States have had a magnetic strip on them since the 1980s. The data standards used to store information on the magnetic strip were fairly open and could be read with an inexpensive reader and software on the internet. Data stored in the card strip has historically not been encrypted. So, there are many cases where credit card data can be stolen when you swipe your card at your favorite store or at a gas pump. Many people have installed "skimmers" at these locations that attach to the card reader and collect credit card data.

However, the big retail issues you have read about in the news involve a failure in one of two areas. One area of concern is that malware was installed in point-of-sale computer systems that could intercept credit card data before it is stored in an encrypted storage location. The other area of concern involved retailers that didn't have properly encrypted storage locations that became compromised.

Historically, credit cards have been like everything else technology-wise: security was an afterthought until it was compromised. What are the new technologies on the forefront of securing credit cards? There are two primary technologies: Smart Cards and Near Field Communication (NFC).

Smart Cards have actually been in use for credit cards in Europe since the mid-1990s. They were also used in the early days of Digital Satellite Television (ex. Dish Network & DirecTV) to confirm your subscription plan and what channels you were allowed to access. Miniature versions of them are the SIM card that is in your cell phone. However, early versions of smart cards could be compromised just as easily as the magnetic strip because the data was not encrypted. Since these cards are programmable and can contain more data than a magnetic strip, they can contain encrypted data secured with a key issued by the bank that owns the card.

So why has the United States not moved to this technology? It appears most banks historically have accepted the risk of fraudulent transactions. Since banks would accept that risk, retailers did not have an incentive to replace their credit card reader infrastructure. However, with the recent big data thefts, card issuers and banks are shifting that risk to retailers and transaction processors. In October 2015, more liability for card-present fraud will be on retailers and transaction processors that are not using smart cards and encrypted transaction processing. Next time you are at your favorite store, see if their credit card readers have a new slot for processing smart cards. While they may not be active, many retailers are getting the infrastructure in place.

How do smart cards compare to Near Field Communication (NFC)? Near Field Communication (NFC) is actually a wireless technology where credit card data is stored on your smartphone. As long as proper encryption is used in your smartphone hardware and software, these transactions can be considered secure. Google Wallet was an early adopter of this technology on some Android smartphones. Apple Pay has just come out for the iPhone 6 and iWatch. Both use this technology, and many experts are touting that the encryption with Apple Pay is superb. It is unknown at this time if this data is also stored in iCloud. If it is, that will make the iCloud service a high-value hacking target in the future.

Before there was NFC, you may have seen or heard about credit cards that you could just wave at a credit card reader. Those credit cards were actually using an RFID chip. However, that technology is well known to be hackable and appears to be fading away.

So, what technology will we use in the long term for credit cards? Magnetic Strip, Smart Cards, NFC? Time will tell which technology will win. It may not be a case of the most convenient technology winning out but rather which technology outlasts hackers the best.

This month's contributor to Consultant's Corner is Charles Smith
Consultant, Cyber Security Services
charles.smith@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
October 2015 / Volume 49

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