# The Global Cyber Advisor

by the Cyber Security Services Group

Schneider Electric

November 2015
Volume 50


**After Paris, new worries over electrical grid attack (EU)**

*From www.usatoday.com, 11/22/2015*

The potential for a devastating attack on the U.S. electricity grid remains high on the minds of utility and government leaders, especially in light of the deadly terrorist actions in Paris on Nov. 13. Just days after the carnage in the French capital, the North American Electric Reliability Corporation (NERC) conducted a massive exercise simulating coordinated assaults on the grid in the U.S., Canada, and Mexico, one that involved cyber and physical attacks that left millions of people without electricity for an extended period of time. The scheduling of the Nov. 18-19 grid-security exercise was coincidental; it had been in the works for months. But Gerry Cauley, the president and chief executive of NERC, said the attacks on restaurants and a concert hall in Paris "heightened awareness" of the risks facing the grid and other infrastructure, including the potential for "explosive devices and shootings" bringing down power plants, substations, and transmission lines.

## this issue



## The Cost of Cyber Crime

Cyber security is a growing international concern. Cyber crime already costs the U.S. about $100 billion annually (weforum.org), and according to the 2015 Global Risks report, the global risks that North America is least prepared for are cyber attacks and failure of critical infrastructure. The impact of cyber crime costs the global economy over $500 billion a year, with some estimates as high as $1 trillion. These are staggering figures, yet looking at the breakdown of an average cyber attack, one can see where these dollars come from[1]:

- $15 million—average annualized cost of cybercrime incurred by an organization
- 46 days—the average time to resolve a cyber attack
- $1.9 million—average cost incurred to resolve a single attack

All of these numbers have increased since last year, yet many companies appear to be resolved to this fate. Over 75 percent say they have had or expect to have such an incident that results in negative public opinion. Other negative impacts of a cyber attack range from loss of reputation, loss or theft of sensitive and confidential information, and potential regulatory fines and/or lawsuits.

Cyber crime is a growing global business. Yet many ask, "What do cyber criminals want from my company?" It's simple—whatever you have. With the growth of nation-state attacks, cyber espionage, and cyber terrorists, the answer typically lies within your industry. Many nation-state attacks originate from developing countries that are interested in growing their critical infrastructure (power, chemical, water, oil/gas), so why not look at successful companies and how they design and operate their systems? Cyber espionage is a growing area of corporate theft, because businesses want to know how their competitors are growing their businesses. Cyber terrorism is also becoming more popular, as cyber terrorists often target companies to disrupt their business with a political agenda.

All industries will fall victim to cyber crimes, but to different extents. The cost of cyber crime will be higher for industries identified as critical infrastructure—energy, utilities, chemical, water, and oil/gas. There is no mistaking it. The direct financial losses associated with a cyber crime can only be equaled by the cost of remediation. The old saying that the best offense is a great defense holds true for cyber security. A comprehensive cyber security strategy will help establish a strong security posture that will in turn moderate the cost of cyber attacks.


[1]Ponemon Institute, 2015 Cost of Cyber Crime Study

# Cyber Central

## NIST Framework for Improving Critical Infrastructure Cyber Security

In September, 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.

We also discussed the Framework Implementation Tiers, which 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]

This 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. Because many organizations are complex and have different functions and roles within the critical infrastructure, they may have a variety of Profiles. A comparison of current and target Profiles can help identify cyber security gaps and establish a plan to address them.[2]

Since the Framework is based on over 320 security standards, it also proves to be very adaptive. The following tables help quantify the ease at which the Framework can be applied to both an organization with no cyber security program as well as an organization with an existing cyber security program.

| NIST Framework Core | NERC CIP Cyber Security Standard |
|---|---|
| Identify | NERC CIP-002 |
| Protect | NERC CIP-003, CIP-004, CIP-005, CIP-006, CIP-007 |
| Detect | NERC CIP-008 |
| Respond | NERC CIP-008 |
| Recover | NERC CIP-009 |


Schneider Electric

# Cyber Central

## NIST Framework for Improving Critical Infrastructure Cyber Security

| Framework | No Existing Cyber Security Program | Existing Cyber Security Program |
|---|---|---|
| **Tier Level** | • What kind of risk and/or security program do you currently have? | • What kind of risk and/or security programs do you currently have? |
| **Core Functions** | • What controls do you currently have?<br>• Review Core Function concepts | • What controls do you currently have?<br>• Review Core Function concepts, mapped to existing standards/requirements |
| **Current Profile** | • Establish a concept profile | • Review current profile, assessment reports, gap analysis, etc. |
| **Target Profile** | • Where would you like to be? | • Where would you like to be? Compliance? |
| **Assessment** | • Clearly define current profile<br>• Create roadmap to target profile(s) | • Create roadmap to target profile(s)<br>• Define remediation scope for defined findings/gaps |

Although the Framework was initially designed for Critical Infrastructure industries, it is readily applicable to any company, no matter its size or industry or country it is located in. The Framework is a best practice approach to cyber security risk management, offering a common language that can be used across all industries. The primary focus is on risk management through the implementation of the Tiers, helping organizations gauge their progress. Lastly, the Framework offers a continuous improvement process. This is critical since cyber threats evolve as quickly as technology improves.

**References**

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

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


Schneider Electric

The Global Cyber Advisor
Cyber Security Services
November 2015 / Volume 50

# Industry News

## Oil and gas pipeline safety market estimated to grow at a CAGR of 7.17% (NA)

*From www.whatech.com, 11/2/2015*

According to the Global Oil and Gas Pipeline Safety Market 2015-2019 report, governments throughout the world are implementing strict regulations in the oil and gas industry. Adhering to these regulations is increasingly becoming mandatory for the oil and gas companies. The analysts forecast global oil and gas pipeline safety market to grow at a CAGR of 7.17% in terms of revenue over the period 2014-2019.

## Obama warns of power grid's lagging cyber defenses (NA)

*From thehill.com, 11/1/2015*

The U.S. isn't spending enough to defend its power grid from cyberattacks, President Obama warned as he declared November Critical Infrastructure Security and Resilience Month. The move is part of the administration's efforts to promote better funding for the nation's roads, bridges, tunnels, power grids and energy systems. Lagging investments in power grids and energy systems, especially, have been increasingly singled out as a looming danger by the White House, presidential candidates, lawmakers and private sector security experts. The inattention has left these networks exposed to potentially catastrophic cyberattacks that could cause massive blackouts and leave people with basic services or resources, they all warn.

## Middle East is not prepared for a major cyber attack (MENA)

*From www.thenational.ae, 11/4/2015*

Governments in the region did not take cyber security seriously a few years ago. Now, after a drumbeat of public revelations of networks being penetrated around the world, many governments in the region have created cyber security systems and programs. Middle East governments, however, did not learn from the mistakes made in the United States, Europe, and Asia. Just like the countries that were early adopters, Middle East governments have placed their initial focus on offensive capabilities and, to a lesser extent, on securing some government networks (chiefly those involved in security). What has been left largely undefended are private sector companies, infrastructure operators, and civilian ministries. Yet they are the most frequent targets for sophisticated hackers seeking to steal money, identity, intellectual property, and valuable financial information. Moreover, it is by attacking the infrastructure operators that an enemy could cripple an economy or a nation.

## Oil industry more exposed to cyber attacks than ever

*From sputniknews.com, 11/18/2015*

It's not just domestic objects that could fall foul to cyber threats; one of the world's largest energy industries could too. The Internet of Things can infiltrate oil production leaving the industry vulnerable to hack attacks. But while the oil and gas industry focus on the slump in oil prices, production, as well as profits, the threat posed by hackers remains underreported. According to Alexander Polyakov, founder of ERPscan a cyber security software firm, the oil and gas industry is "a juicy target for cyber attacks as oil and gas companies are responsible for a great part of some countries' economy."

## UK pummeled with DDoS after ISIS cyber attack warning (EU)

*From www.telecomstechnews.com, 11/18/2015*

Earlier this month, the UK government warned ISIS militants were developing the capability to launch cyber attacks against Britain's infrastructure. Now, we are witnessing a huge amount of DDoS (Distributed Denial of Service) attacks on the United Kingdom. As of writing, a look at the Digital Attack Map shows an unprecedented amount of attack traffic aiming towards the UK. Most of the DDoS attacks use "fragmentation" which sends a flood of TCP or UDP fragments to a victim, overwhelming the victim's ability to re-assemble the streams and severely reducing performance.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
November 2015 / Volume 50

# Cyber News

## IS hacks 54,000 Twitter accounts to promote propaganda

*From www.middleeasteye.net, 11/9/2015*

Thousands of Twitter accounts were reportedly hacked by the Islamic State group in what members said was revenge for the killing of one of their leading hackers earlier this year by a US drone in Syria. The hacking team, which called itself the Cyber Caliphate, posted its propaganda through 54,000 infiltrated accounts. The apparent mobile numbers of the CIA, FBI and NSA chiefs were also posted, as the group said that it would take years to post all of the seized information.

## Analysts warn Middle East hackers trying to attack US infrastructure

*From www.voanews.com, 11/18/2015*

Security in Washington and across the United States is tightening following a new video reportedly released by Islamic State specifically threatening an attack on the American capital similar to the brutal killings in Paris. But while security officials work to harden potential targets against any terrorist threats, a growing number of cybersecurity analysts are warning some of the most critical U.S. assets are all but unprotected: namely the nation's millions of digital operational networks that control everything from water treatment to manufacturing to the electric grid. Even more ominously, there are new indications the fastest growing cyber threat is coming from hackers based in the Middle East, including regions known to be controlled by IS, and that unless something is done, the United States may soon face what some are calling a "cyber Pearl Harbor."

## One in five UK bank accounts hacked through cyber attacks

*From www.ischoolguide.com, 11/24/2015*

According to new research from business advisory firm Deloitte, one in five UK bank accounts have been breached from cyber attacks. Banking Technology reported that 21% of consumers had their personal details stolen including their bank accounts, and were used to buy goods and services. According to Independent, in a survey of nearly 1,500 UK consumers, over 70 percent would think twice on being with a company if it failed to keep their personal information safe. As per the Deloitte report entitled "Consumer Data Under Attack: The Growing Threat of Cybercrime," they found out that 41% of respondents in the consumer sector said that they feel that they are being targeted by cyber criminals. 39% had their personal data stolen, which is a big raise from 2013's 26%.

## Australia vulnerable to a cyber attack disaster

*From www.smh.com.au, 11/13/2015*

Australian government agencies and organizations are increasingly vulnerable to a major cyber attack yet security has not evolved in more than 20 years, according to an international cybercrime expert. Chris Pogue, a member of the US Secret Service Electronic Crimes Task Force, will conduct high-level security briefings with government departments and security agencies in Canberra to urge better collaboration and intelligence sharing in the face of an "inevitable" cyber disaster. With the trade of stolen data booming on the multi billion-dollar dark web, Mr. Pogue said "data is the new oil" yet Australia, like most countries, still has a "head-in-the-sand approach."

## 39% of large businesses risk take up to a month to close dormant accounts

*From www.information-age.com, 11/11/2015*

More than a third (39%) of large British businesses take between a few days and a month to close dormant accounts of former employees, research has revealed. Doing so leaves them more open to a cyber attack, according to Ilex International, which conducted the study with YouGov. A quarter (24%) of respondents from large businesses terminated access to dormant accounts 'a few days after departure', 5% waited up to a week and 3% within a fortnight, while 8% confessed to only removing access within a month. Immediate termination on or before the day of departure is even worse for small and medium size businesses, bringing the total number of respondents following this best practice down to 32% and 56% respectively.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
November 2015 / Volume 50

# Cyber exploit capabilities grow as digital mercenaries enter the arena

Recently, Jane's Intelligence Review, an online and published industrial journal specializing in Defense topics published an article that heralded the growth of cyber mercenaries. The gist of the article is that information is king and that it's desirable for governmental (and corporate) entities not to use governmental assets for the purpose of plausible deniability while engaged in cyber exploration, espionage, and attack. The cyber mercenaries, a new service-oriented industry, have entered this niche and utilize increasingly more sophisticated successively developed tools on for-hire basis.

It's very difficult to associate a smoking gun with a particular attacker. Recently, NTT published their 2015 Global Threat Intelligence Report. In their report they indicated that "56% of the attacks against the NTT global client base originated from an IP address with in the United States." Gone are the days where you go to the Internet registries and block those groups of IP addresses at your internet point of presence for regions that you are unlikely to conduct business with. NTT attributed the popularity of the United States for an attack presence to the availability of network resources and computers for attackers to use.

Tying the two articles together, professional non-governmental black hat for-profit organizations are utilizing bot nets comprised of poorly secured and patched home-based equipment to perform contract-to-extract attacks against more secure targets. NTT indicated that most targeted exploits against commercial entities were using vulnerabilities that were less than a year old. Patching remains the first line of defense. Later in their document they suggest that 76% of the identified vulnerabilities in an enterprise were more than 2 years old, suggesting poor compliance with patching.

Consider the impact to a California health care provider whose insurer challenged the claims of the provider in court related to a HIPAA breach because the insured refused to systematically conform to developed internal controls. The insurer stated that the insured failed to regularly "re-assess its information security exposure and enhance risk controls" and to "deploy a system to detect unauthorized access or attempts to access sensitive information stored on its servers." The same article suggests that cyber insurance is growing yearly at 38% and, of course, insurance is not in the business of paying claims.

The requirement to conduct regular re-assessments is implicit. Embedded in the insurer's defense is that the suggestion that the insured is required to have an intrusion detection system (IDS)/logging and alerting system. Intrusion Detection Systems inspect network traffic for anomalous network traffic behavior. This becomes more complex, as there are two forms of IDS, behavioral and signature-based. Signature-based is more common in that it's like anti-virus definitions—as the exploits are recognized, the manufacturer publishes an update to the signature, which keys off of particular aspects of the attack. Behavioral relies on knowing what normal behavior is between different systems in your implementation to recognize anomalous behavior. Corporate staff need to be comfortable analyzing network protocols in order to determine the flagged behavior. However, with the signature version, if the attack hasn't been recognized, analyzed, and distributed by the vendor, no tree falls in the forest. Some entities find an installation of each complementary depending on their budget. Depending on the level of experience of the staff and the entity's appetite for risk, this may be a service worth outsourcing based upon perceived liability.

This month's contributor to Consultant's Corner is David Milne
Consultant, Cyber Security Services
david.milne@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
November 2015 / Volume 50

# 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