The Global Cyber Advisor

by the Cyber Security Services Group

Schneider Electric

September 2015
Volume 48

OPM says 5.6 million fingerprints stolen in cyber attack

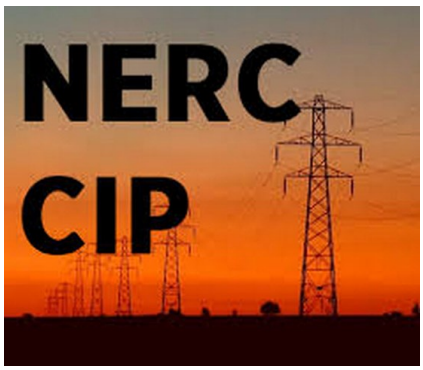
From www.washingtonpost.com, 9/23/2015

One of the scariest parts of the massive cybersecurity breaches at the Office of Personnel Management just got worse: The agency now says 5.6 million people's fingerprints were stolen as part of the hacks. That's more than five times the 1.1 million government officials estimated when the cyberattacks were initially disclosed over the summer. The total number of those believed to be caught up in the breaches, which included the theft of the Social Security numbers and addresses of more than 21 million former and current government employees, remains the same.

this issue

- NERC CIP V6 — Here We Are Again
- Cyber Central
- Industry News
- Cyber News
- Consultant's Corner

NERC CIP V6 – Here We Are Again



No sooner had the ink dried on NERC CIP V5 (Nov 2013) there was talk about a V6 and V7. Well, wait no more—the Federal Energy Regulatory Commission (FERC) has filed a Notice of Proposed Rulemaking (NOPR) that proposes changes to V5. The North American Electric Reliability Corporation (NERC) is overseen by FERC and implements the Critical Infrastructure Protection (CIP) standards to govern the cyber and physical security of the bulk electric system. These CIP standards are mandatory and enforceable and any utility that violates these standards are subject to fines.

The basic drivers for the new NOPR is a growing concern by FERC of the increasing malware threats that are targeting supply chain vendors and the lack of coverage for these threats in the current CIP standards. FERC also directed NERC to develop enhanced security controls for low impact assets, controls to address the risk of transient electronic devices (i.e., removable media such as thumb drives and laptops), and a clearer definition of the term "communications network."

The proposed changes outline modifications to CIP V5 standards and will be known as CIP V6: CIP-002-6, CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2.

In addition to the proposed modifications, FERC is also proposing new terms:

- Transient Cyber Asset and Removable Media
- Revised BES Cyber Asset (BCA)
- Protected Cyber Asset (PCA)
- Removable Media
- Transient Cyber Asset
- Low Impact BES Cyber System Electronic Access Point (LEAP)
- Low Impact External Routable Connectivity (LERC)

As with previous CIP version updates, there is much speculation in regards to what the final document will look like. FERC has made a lot of headway with the previous CIP versions and there is little reason to believe that these changes will continue to provide the regulatory guidance that is relevant to today's threats and will keep our critical infrastructure secure.

Cyber Security Services by Schneider Electric

September 2015 / Volume 48

Cyber Central

NIST Framework for Improving Critical Infrastructure Cyber Security

Cyber threats to global critical infrastructure are continuing to increase. Reports by ICS-CERT[1] show that the Energy, Critical Manufacturing, and Water industries have the greatest number of cyber threats, despite the fact that these industries are under increasing pressure from regulatory standards from governments and regional entities. The NIST Framework is not prescriptive, but rather complements and does not replace an organization's existing business or cyber security risk management process and cyber security program. Instead, the organization can use its current processes and leverage the framework to identify opportunities to improve an organization's cyber security risk management. Alternatively, an organization without an existing cyber security program can use the Framework as a reference when establishing one. Most importantly, the NIST Framework is versatile enough that it can be used in lesser-regulated industries anywhere in the world.

The NIST Framework is not a checklist or a list of requirements like other standards. Instead, it is based on three tenets, the Framework Core, the Framework Profile, and the Framework Implementation. 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 a unique identifier to the different elements:[2]

Function	Category	Subcategory	Informative Reference(s)
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Identify: Develop the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities.

Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect: Develop and implement the appropriate activities to identify the occurrence of a cyber security event.

Respond: Develop and implement the appropriate activities to take action regarding a detected cyber security event.

Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event.

The NIST Framework structure and language does not require cyber security expertise and is as easily understood in the C-Suite as it is on the manufacturing floor. 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.

Next month we will discuss the Framework Implementation Tiers, which helps organizations rate their cyber security readiness based on four levels of maturity..

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
September 2015 / Volume 48

Industry News

Energy Department struck by cyber attacks (NA)
From www.usatoday.com, 9/11/2015

Cyber attackers successfully compromised the security of U.S. Department of Energy computer systems more than 150 times between 2010 and 2014, according to a review of federal records obtained by USA TODAY. Incident reports submitted by federal officials and contractors since late 2010 to the Energy Department's Joint Cybersecurity Coordination Center shows a near-consistent barrage of attempts to breach the security of critical information systems that contain sensitive data about the nation's power grid, nuclear weapons stockpile and energy labs. The records, obtained by USA TODAY through the Freedom of Information Act, show DOE components reported a total of 1,131 cyberattacks over a 48-month period ending in October 2014. Of those attempted cyber intrusions, 159 were successful.

US power grid getting hammered (NA)
From thehill.com, 9/9/2015

Critical infrastructure operators in the U.S. continue to face a hailstorm of hacks. Federal documents obtained by USA Today through a FOIA request revealed that hackers infiltrated the Department of Energy's computer system over 150 times between 2010 and 2014. As the department overseeing the country's power grid and nuclear weapons stockpile, the Energy Department is an attractive target for overseas cyber spies seeking to uncover vulnerabilities. Meanwhile, the Department of Homeland Security is warning critical infrastructure providers of a malicious spear-phishing campaign in which hackers use bogus emails to infiltrate users' networks. The campaign has targeted government facilities and chemical, critical manufacturing and energy companies.

Most cyber attacks against Iran are launched from Israel (MENA)
From en.trend.az, 9/9/2015

Each day 10,000 Internet security incidents are detected in Iran and the country ranks 19th in terms of cyber security, a new report says. Iran has accomplished only 39 percent of a target 53 percent of its Information Security Management System (ISMS) and 20 percent of a target 100 percent for launching a Security Operation Center SOC , the report by Mehr news agency said. IT Minister Mahmoud Vaezi has said most of cyber-attacks against Iran are launched from Israel. According to Vaezi, a number of Western and Arab countries rank behind Israel in launching cyber-attacks on Iran.

Industrial cyber security awareness stays low despite high profile silent attacks (EU)
From www.voltimum.co.uk, 9/16/2015

As the Internet of Things (IoT) transforms plant and other architectures, defense-by-default security strategies will give way to defense-by-design solutions. So says a new report by market analysts Frost & Sullivan. Today's vast proliferation of digital networks and devices, varying communication channels, and the use of off-the-shelf software has made cyber security an absolutely crucially important consideration. This is particularly so now that the IoT and the Industrial Internet of Things (IIoT) are proliferating at a huge rate, with the IoT alone predicted to have – at a very conservative estimate – 20 to 50 billion devices connected to the Internet by 2020. Safety and security concerns associated with the high levels of connectivity and integration are surfacing as the IoT takes shape in industrial networks and manufacturing plant floors to become the IIoT.

Homeland Security websites vulnerable to cyber attacks (NA)
From www.newsweek.com, 9/15/2015

The U.S. department charged with protecting government computers needs to secure its own information systems better, according to an audit released on Tuesday that showed lapses in internal systems used by the Secret Service and Immigration and Customs Enforcement. The Department of Homeland Security also needs to establish a cyber training program for analysts and investigators, the audit said, with officials from several agencies blaming short-term budget allocations from Congress for their training cuts. "We identified vulnerabilities on internal websites at ICE and USSS that may allow unauthorized individuals to gain access to sensitive data," according to the report by the Office of the Inspector General for DHS.

Developing an Australian cybersecurity framework (APAC)
From www.businessspectator.com.au, 9/18/2015

The Australian government is developing a framework for how Australia should best address electronic threats and the US NIST Cybersecurity Framework offers some pointers as to what approach may be best suited for the task. The Australian Cyber Security Centre (ACSC) has been busy since it was announced in late 2014, with Australia's first cybersecurity conference, held in Canberra in April, it's first big event. The conference, attended by over 700 security experts from Australia and abroad, was well attended, highlighting how critical the issue of cybersecurity has become in Australia in recent years.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
September 2015 / Volume 48

Cyber News

Companies lose $400 billion to hackers each year

From www.inc.com, 9/30/2015

Cybercriminals are pilfering a staggering volume of data and money from companies around the world. The damage from hacks costs businesses $400 billion a year, according to British insurance company Lloyd's. Even worse, a significant portion of cybercrime goes undetected or unreported, a World Economic Forum (WEF) report finds. Companies often prefer to say nothing than to open themselves up to legal action, trouble with regulators, and damage to their reputation.

Cyber attacks could cost up to $90 trillion by 2030

From www.washingtonexaminer.com, 9/11/2015

Cyberattacks dragging down the Internet could cost the world up to $90 trillion by 2030, according to a new study, unless cyber security advances at a rapid pace. The study, published by the Atlantic Council and the Zurich Insurance Group, notes that the world could derive up to $190 trillion in economic benefit in a best-case scenario. "Tens and even hundreds of trillions of dollars are at stake," the authors state, or "nearly 10 percent of total global GDP."

NSA chief says Iranian cyber attacks against US have slowed

From www.wsj.com, 9/10/2015

Cyber attacks against the U.S. by Iranian hackers have eased noticeably since nuclear talks intensified last year, but there is no sign that Iran's leaders plan to scuttle their cyber weapons program, National Security Agency Director Adm. Michael Rogers said. At a House Intelligence Committee hearing, Adm. Rogers said there was "significant Iranian activity" related to cyber attacks against U.S. financial firms a couple of years ago. Director of National Intelligence James Clapper added that Iran and North Korea are among a tier of nation states that have advanced cyber weapons, though they are considered unpredictable in how they use them.

Cyber security expertise in high demand as threats increase

From www.itproportal.com, 9/15/2015

It seems a growing number of businesses are seeking cyber security expertise as jobs in the area now make up 14 per cent of all new UK-based IT roles. This is according to new research by professional services consultancy Procorre, which also claims 15 percent of cyber security roles pay over £100,000. The firm claims that this growing interest in professionals in this area is the result of recent high profile hacks that exposed the vulnerability of many businesses' IT security systems and the extent of the potential threat.

Cyber attacks from Middle East increasing

From www.nationaldefensemagazine,org, 9/16/2015

Cyber attacks originating from Middle Eastern countries such as Syria and Iran are expected to increase over the next several years, said one defense expert. "The reason that the cyber attacks are happening is because of events that are happening on the ground in the region," said Terry Pattar, a senior consultant at IHS' aerospace, defense and security division. "The three main drivers … [are] the Syrian civil war, the 'cold war,' as it's termed with Iran, and the long standing enmity between Israel and … countries and parties in the region." These threats have increased significantly over the past year, Pattar said during a speech at the Defense and Security Equipment International conference. A large portion of these attacks have come from the Islamic State — the most active militants online — which has at least two hacking groups.

Cyber attacks cost global business over £200bn a year

From www.cityam.com, 9/22/2015

Cybercrime is hitting businesses hard, with attacks costing billions every year, and the finance sector is worst exposed as one in four businesses were victims of attacks in the past year. Some 15 per cent of businesses have faced a cyber attack in the past year, with the EU region hit worst, global survey Grant Thornton International Business Report reveals. The attacks are costing global business over £200bn a year, with the financial industry bearing the brunt of the weight.

Cyber security market expected to reach $170.21 billion by 2020

From www.whatech.com, 9/22/2015

MarketsandMarkets expects the global cyber security Market to grow from $106.32 Billion in 2015 to $170.21 Billion by 2020, at a Compound Annual Growth Rate (CAGR) of 9.8%. In the current scenario, North America is expected to be the largest market on the basis of spending and adoption of cyber security solutions and services.

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
September 2015 / Volume 48

Why is Cyber Security Important?

Cyber Security is the generic term used to describe many different areas of protecting networks. The problem with cyber security is the ever-changing arena. Malware created years ago were relatively simple attacks. In the past, anti-virus software was the typical protection used to minimize loss from a cyber attack. Unfortunately, cyber attackers have become much more sophisticated. A point solution like anti-virus software or a firewall for cyber security protection is now inadequate in the current threat landscape.

A multiple-approach method is required to minimize the current cyber security threat. Malware is now just one of the potential issues. Bots (imbedded malicious code) can turn over control of your computer to a malicious attacker. Phishing and targeted personnel attacks are becoming extremely prevalent (the attackers are now correctly spelling—or have figured out how to use spell check—on the attack emails). Social engineering is being used to identify information to assist in an attack. So, firewall and authentication methods are circumvented when the attacker has acquired the proper username and password.

Vulnerabilities in software and hardware provide an additional attack vector. Software updates and patches are critically important. Hardware updates are required to minimize the known hardware attacks.

With the plethora of different attack vectors, multiple methods are necessary to thwart the multiple vectors. Simple authentication is not enough; multi-factor authentication is necessary. Firewalls blocking IP addresses and ports are inadequate. The next generation of firewalls now block based on applications used, location of source, specific MAC address of sender, and even a sender-provided token to match the receiver token.

Cyber Security training for all personnel is critical. Many attacks use social engineered information (a dog's name from a social media site) to determine a password. Complex algorithms have been created to skim social media for potential user information to provide clues for passwords or user names. Informing employees of the creative ways attackers acquire personal information is required to change personal habits.

All the information above is a brief synopsis of how a multi-layered approach is required to secure your information. Training, hardware, malware protection, traffic monitoring, information logging, and the proper architecture are all parts of the multi-faceted approach to Cyber Security. Unfortunately, out-of-the-box solutions, like the unicorn, are a mythical thing. Continuous effort is required to minimize the cyber security threats and will require continuous improvements. Unfortunately, there are many unscrupulous individuals with motivation to acquire someone's information or data. We must be vigilant to protect the important information or be prepared for the negative impact of an unscrupulous individual or group using important information.

This month's contributor to Consultant's Corner is Bernie Pella
Consultant, Cyber Security Services
bernie.pella@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Cyber Security Services
September 2015 / Volume 48

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