SEARCHSECURITY.COM

technical guide on NERC COMPLIANCE

contents

TechTarget

3 Critical questions

- How secure & compliant is my network?
- Which top issues must we address today?
- Who is accountable & how are they doing?

1 Suite answer

nCircle Suite360™

The Leader in Security & Compliance Auditing

Download whitepaper to get started with NERC CIP compliance
www.ncircle.com/NERC

nCircle

insight

NERC COMPLIANCE

The United States' electric grid is under scrutiny from regulators and under attack by criminal hackers and foreign enemies. These elements are exploiting weaknesses inherent in critical infrastructure that can no longer be ignored.

SEARCHSECURITY.COM presents a comprehensive guide to NERC compliance. Our experts cover all the angles in order to help your efforts in meeting compliance with the information security standards established by the North American Electric Reliability Corporation.

contents

Even Angels Fear To Tread Where NERC CIP Compliance is Involved

> With astronomical fines looming, utilities can no longer rely on the first generation NERC CIP compliance solutions that were rushed to meet deadlines.

By Jasvir Gill, Founder & CEO, AlertEnterprise, Inc.

The evolving requirements for NERC CIP Compliance have made it impossible for controls documentation solutions to automate new requirements like tracking training and certifications for employees, instantly removing physical access for terminated employees, and monitoring contractor access. How many systems, databases and logs will you have to scan to find out which terminated employees have active access to SCADA or physical access to remote substations? The answer is an important one, since knowing this is now a mandate.

Click here to see a screen shot of AlertEnterprise's NERC CIP solution used to identify and remove terminated employees' access to SCADA

Weighted down by the crushing burden to deliver documentation and evidence, sometimes we forget that the ulitmate goal is security and reliability. True security can only be achieved with a combination of compliance and active policy enforcement. Security, risk and compliance is managed in silos today - even in the best of organizations. IT security, control systems engineers and physical security teams rely on a variety of applications and systems. Organizations are being forced to rely on manual processes to bridge the gaps between them.

A new breed of NERC CIP compliance applications to the rescue - conducting risk analysis across multiple enterprise applications, security applications and regulations is a daunting challenge hindered by the sheer complexity of the underlying tools that extend across multiple vendors and into the physical security domain.

This integration is needed to truly address all facets of NERC CIP. Organizations will no longer be stuck using their software tools for "documentation only" and then manage evidence separately to meet the demands of auditors, or rely on physical security to turn off badge access at some time in the future, when they get around to it. The new generation of compliance solutions deliver total compliance automation as well as prevention of sabotage and malicious acts that could compromise reliability. An integrated software solution manages background checks and certifications for employees and contractors and determines access rights to operational applications like EMS, DMS, enterprise applications (SAP and Oracle), IT systems, facilities, secured perimeters and control systems.

Jasvir Gill, CEO, AlertEnterprise, holding up the Most Innovative Cyber Security Company trophy awarded to his company at the RSA Security Conference.

Jasvir Gill is the Founder and CEO of AlertEnterprise. An early pioneer in establishing GRC as a software market segment, Jasvir was also the Founder & CEO of Virsa Systems which was acquired by SAP. *jasvir@alertenterprise.com*

Situational awareness and incident management capabilities can be leveraged to monitor insider threat, track operator actions in control rooms and even detect potential sabotage directed against remote assets like substations. Just imagine being able to track the entry of a maintenance employee into a remote substation and the subsequent departure following the visit, only to detect that employee forgot to enable the protective relay following the repair task. The sofware recognizes the sequence of events and based on rules, notifies the control room. Major blackout averted, millions of dollars in fines avoided

STANDARDS

Getting to Know the NERC CIP Standards

Learn what you need to know about the NERC CIP standards.

BY ERNIE HAYDEN

THERE'S BEEN A lot of buzz in the news lately about the new security regulations that electric utilities need to meet. In this article, we'll cover what utilities need to know and do to become compliant.

What is NERC? What is FERC?

These rules have been mandated by the Federal Energy Regulatory Commission (FERC)—a Federal organization overseeing interstate transportation and marketing of energy. In turn, these requirements are being written and enforced by the North American Electric Reliability Corporation (NERC) and associated regional coordinating councils, with substantial input from the utilities themselves. NERC is headquartered in Princeton, N.J., and is an international, independent, self-regulatory, not-for-profit organization, whose mission is to ensure the reliability of the bulk power system in North America.

The nine rules being imposed are called the NERC Critical Infrastructure Protection (CIP) standards and are often referred to as NERC CIP-001 to CIP-009. The standards constitute about 47 requirements and approximately 100 sub-requirements.

The standards are organized by topic as follows:

- CIP-001 – Sabotage reporting
- CIP-002 – Critical cyber asset identification
- CIP-003 – Security management controls
- CIP-004 – Personnel and training
- CIP-005 – Electronic security perimeters
- CIP-006 – Physical security of critical cyber assets
- CIP-007 – Systems security management
- CIP-008 – Incident reporting and response planning
- CIP-009 – Recovery plans for critical cyber assets

The overriding goal of CIP-002 through CIP-009 (CIP-001 generally isn't tied to cybersecurity) is to ensure the bulk electric system is protected from unwanted and destructive effects caused by cyberterrorism and other cyberattacks, including attacks from within the utility (i.e., insider threats). Essentially, FERC—through NERC—wants assurance that the main electric grid in North America will not fail due to cyber-related

vulnerabilities and subsequent attacks.

The bulk electric system includes electrical generation resources, transmission lines, interconnections with neighboring electric grids, and associated equipment, generally operated at voltages of 100,000 volts or higher. Large transmission towers and the huge substations on the transmission grid are part of the bulk electric system. However, the distribution power lines and equipment—operating at a much lower voltage in neighborhoods—are not included in the NERC CIP standards.

To ensure that utilities and affected electric energy companies are focused on the right systems, the NERC CIP standards offer a sequenced approach to identifying critical cyberassets. But companies must first understand what their "critical" assets are. These are facilities, systems and equipment which, if destroyed, degraded or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system. These assets normally include system control centers, large generation facilities and critical substations, to name a few.

Companies then must closely examine these critical assets and identify the cyber aspects that could directly affect the more general critical assets in the event of a hacking or failure. Such an event could result in a negative impact to the critical asset, and eventually cascade to the bulk electric system.

This represents an opportunity for solution providers, as some utilities may need assistance with creating this asset inventory and identifying the "critical assets."

NERC CIP standard opportunities for solution providers

The standards themselves are primarily focused on programs and processes and not so much on implementing specific technologies. Interestingly enough, most Supervisory Control and Data Acquisition (SCADA) systems are on the "edge" of inclusion in the NERC CIP standards because they tend to operate in layer 2 of the OSI model, whereas, the primary focus of the NERC CIP standards is on those systems that are TCP/IP or layer 3-based.

Many utilities will need assistance with system penetration and vulnerability testing of the critical cyber assets, as well as cyber systems used to provide physical protection of critical cyber assets. In these cases, a utility may be interested in assistance from a trained and experienced solution provider to provide the vulnerability testing, and detailed reports for audits.

The NERC CIP standards needed to be implemented by June 30, 2009 for substations, system control centers and other affected systems except for electricity generation assets. The generation assets must be compliant by Dec. 31, 2009. In addition to these deadlines, the NERC regional entities are now performing spot checks (essentially a limited audit) at utilities with a narrow focus on the first 13 standards that needed to be fulfilled in 2008 for system control centers.

Right now, most utilities are moving at break-neck speed to ensure they are compliant with NERC CIP standards. Their primary motivation is that NERC may—and has—imposed fines on utilities for non-compliance with the NERC CIP standards.

The primary way solution providers can help the utilities is by assisting them in implementing what I call "holistic, pragmatic security," and that can include a number

of things. Some need help writing policies, standards and procedures that meet the NERC CIP standards. Other utilities need help with establishment of Electronic Security Perimeters (from CIP-005) with firewalls and other perimeter technologies. Still other utilities need help with personnel training and personnel background checks as well as strong, well organized physical and logical access control systems (CIP-004, CIP-006 and CIP-007).

Overall, this is just the beginning for the electric energy sector. NERC continues to provide reports on its audit findings and deliver analyses of electric grid events to FERC. Version 3 of the NERC CIP standards is currently under development, and will focus on inclusion of the level-2 SCADA protocols, encryption of communications, forensics following a cyber incident and closer alignment with the National Institute of Science and Technology (NIST) standards for cyber security. These future areas of inclusion for the CIP standards may be an area where security solution providers can assist utilities in their compliance activities going forward, as they can help lead utilities in developing information and infrastructure security programs that more closely resemble some programs in place in other industries. Regardless, revised standards are already expected in 2010 or 2011.

What's next? Hold on to your hat!

Ernie Hayden is the former CISO for the Port of Seattle, Group Health Cooperative and most recently Seattle City Light where he coordinated the efforts regarding NERC Critical Infrastructure Protection compliance. Hayden holds a CISSP and a Certified Ethical Hacker and lives in the Seattle area.

ASSET IDENTIFICATION

NERC CIP Training: Understanding 'Critical Cyber Asset Identification'

To pass critical infrastructure protection standards, utilities must ensure that all critical and cyber assets are identified and protected. BY ERNIE HAYDEN

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009 provide the minimum requirements for utilities and other affected enterprises to ensure the Bulk Electric System (BES) is effectively protected from cyberattacks and faults.

To be successful in the entire implementation of the NERC CIPs, a utility must ensure that all critical assets and Critical Cyber Assets (CCAs) are properly identified and then properly protected. Therefore, it is an operational imperative to those covered by the NERC CIPs to get CIP-002 done right the first time.

Before diving into the CIP-002 requirements and how to take the right actions, some key terms need to be defined and highlighted to help you better understand this process. These terms are summarized below and defined in the NERC Glossary.

To be successful in the entire implementation of the NERC CIPs, a utility must ensure that all critical assets and Critical Cyber Assets (CCAs) are properly identified and then properly protected.

- **BULK ELECTRIC SYSTEM (BES):** The electrical generation resources, transmission lines, interconnections with neighboring systems and associated equipment, generally operated at voltages of 100 kV or higher. Protecting the BES is the primary focus of the NERC CIPs.
- **CRITICAL ASSETS:** Facilities, systems and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. Examples of critical assets include generating plants, major transmission substations and system control centers.
- **CRITICAL CYBER ASSETS (CCAs):** Programmable electronic devices and communication networks including hardware, software, and data that are essential to the reliable operation of Critical Assets.

Identification of Critical Cyber Assets

CIP-002 mandates utilities follow a high-level approach for Critical Cyber Asset identification. A summary of these steps is as follows:

1. First, the utility must *identify and document* a risk-based methodology to be used to identify its critical assets. An excellent reference to help utilities with this process development is provided by NERC.

2. Second, using the risk-based methodology identified above, the utility shall review all of its assets and then identify its critical ones. This must be done at least annually. Of course, the process must be documented and you are expected to follow the procedure and process prepared in #1.

At a minimum you are expected to consider the following assets:

1. Control centers and backup control centers.
2. Transmission substations important to the BES.
3. Generation resources important to the BES.
4. "Blackstart" resources—i.e., those generators and substations needed if there is a complete system blackout and no electric power is available.
5. Automatic load shedding systems capable of shedding 300 megawatts (MW) or more.
6. Any other asset deemed critical to the reliable operation of the BES.

3. Thirdly, using the list of critical assets you developed in #2, you need to prepare a list of CCAs essential to the operation of the critical asset. Examples at control centers could include cybersystems that provide monitoring and control (e.g., SCADA systems), automatic generation control, real-time power system modeling, and real-time inter-utility data exchange.

Of note, the NERC CIPs mandate that the CCAs must also meet one of the following characteristics. That is, the cyberasset:

1. Uses a "routable protocol" to communicate.
2. Uses a "routable protocol" within a control center.
3. Is dial-up accessible.

To help you better understand the hierarchy of the BES to the Critical Assets to the CCAs, see "Identification of Critical Cyber Assets," above.

Many people are surprised to see that the Critical Cyber Assets are only limited to "routable protocols." The Frequently Asked Questions (FAQs) Cyber Security Standards CIP—002—1 through CIP—009—1, issued by NERC, states: "The Critical Cyber Assets that use non-routable protocols have a limited attack scope; hence, they are less vulnerable than Critical Cyber Assets using routable protocols." This document further notes that "routable protocols" are those that provide switching and routing as described by the Open System Interconnection (OSI) model Layer 3 or higher.

Essential Task

Overall, getting the list of critical assets and Critical Cyber Assets complete and correct is absolutely essential for the enterprise that is required to follow the NERC CIP requirements. This is not an impossible process; however, a utility and its supporting vendors really need to pay close attention to detail in this process to avoid "surprises" later on in the NERC CIP implementation. Even the Chief Security Officer of NERC, Michael Assante, has criticized the industry for its failure to adequately and thoroughly identify their critical assets and CCAs. Therefore, NERC has high expectations for utilities to do this process right the first time.

Handy NERC CIP Training Resources

NERC CIP-002, Critical Cyber Asset Identification Standard

Reliability Standards Audit Worksheet (RSAW) – CIP-002

Frequently Asked Questions CIP-002

NERC Guideline: Identifying Critical Assets

Ontario: NERC Cyber Security Standards – Risk-Based Methodology

Western Electric Coordinating Council (WECC) CIP User Group Presentation

NERC Glossary

Ernie Hayden is the former CISO for the Port of Seattle, Group Health Cooperative and most recently Seattle City Light where he coordinated the efforts regarding NERC Critical Infrastructure Protection compliance. Hayden holds a CISSP and a Certified Ethical Hacker and lives in the Seattle area.

Your One Stop Shop for All Things Security

Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professional. Free.

IT security pro's turn to the TechTarget Security Media Group for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security standard compliance, videos, webcasts, white papers, podcasts, a selection of highly focused security newsletters and more — **all at no cost.**

Feature stories and analysis designed to meet the ever-changing need for information on security technologies and best practices.

INFORMATION SECURITY®

www.SearchSecurity.com

Breaking news, technical tips, security schools and more for enterprise IT professionals.

SearchSecurity.com

www.SearchSecurity.com

Learning materials geared towards ensuring security in high-risk financial environments.

SearchFinancialSecurity.com

www.SearchFinancialSecurity.com

UK-focused case studies and technical advice on the hottest topics in the UK Security industry.

SearchSecurity.co.UK

www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.

SearchMidmarketSecurity.com

www.SearchMidmarketSecurity.com

Technical guidance AND business advice specialized for VARs, IT resellers and systems integrators.

SearchSecurityChannel.com

www.SearchSecurityChannel.com

TechTarget®
The IT Media ROI Experts

INSIDER THREAT

Introduction to NERC CIP 004 Compliance Standards: Training Personnel

Learn how to comply with NERC CIP 004, an electric utility standard that focuses on the insider threat.

BY ERNIE HAYDEN

IN THE PAST YEAR, North American electric utilities have increased their focus on NERC CIP compliance standards. As a reminder, these standards have been issued by the North American Electric Reliability Corporation with emphasis on ensuring the bulk power system—i.e., the main electric transmission grid—is protected from cyberattack.

Of course a cyberattack can come from outsiders, including organized criminals, script kiddies or nation states; however, the NERC CIP 004 standard, in particular, focuses on protecting the grid from the insider threat. This standard helps ensure that personnel who have authorized cyber or authorized unescorted physical access to critical cyber assets (CCAs)—including contractors, service vendors or temporary employees—have been appropriately vetted for their background and have the appropriate level of security training and awareness prior to gaining access to the CCAs.

A survey of the requirements

NERC CIP-004 has four primary requirements that include the following key points:

Requirement 1–Awareness: This requirement mandates that an affected utility establish, maintain and document a security awareness program for those who have "…authorized cyber or authorized unescorted physical access" to critical cyber assets. An awareness program is really a good practice for any company. It will help evangelize expectations for employee security practices regardless of the NERC requirements.

At a minimum, each quarter the utility should reinforce sound security practices—especially for the security of the critical cyber assets—through:

a) direct communications (e.g., emails, memos, computer-based training, etc.)
b) indirect communications (e.g., posters, intranet postings, brochures, etc.)
c) management support and reinforcement (e.g., presentations, meetings, etc.)

Requirement 2–Training: In this requirement, an affected utility must establish, maintain and document an annual cybersecurity training for the same group of employees covered in Requirement 1 (i.e., those with "…authorized cyber or authorized unescorted physical access"). The training should include discussions on the policies,

access controls and procedures developed to protect from damage or hacking of the critical cyber assets. The training should include the following required items:

- Proper use of critical cyber assets.
- Physical and electronic access controls to critical cyber assets.
- Proper handling of critical cyber asset information.
- Action plans and procedures to recover or reestablish critical cyber assets following a cybersecurity incident.

At a minimum, the utility must maintain detailed records showing that the training was performed for each affected individual, at least annually, including the date the training was completed.

At a minimum, the utility must maintain detailed records showing that the training was performed for each affected individual, at least annually, including the date the training was completed.

Most importantly, according to Version 3 of CIP-004, the individuals must be "…trained **prior** to their being granted such access except in specified circumstances such as an emergency." And here, the utility needs to have a documented program that addresses when an emergency access is authorized before the training can be given.

Requirement 3–Personnel risk assessment: The basic premise of this requirement is to ensure a background check has been performed on those individuals electronically accessing or physically touching the critical cyber assets. Some key points about the background checks and their performance are as follows:

- Each background check must include at least identity verification of the individual (e.g., Social Security number verification in the U.S.) and a seven-year criminal check.
- The background checks must be updated at least every seven years after the initial risk assessment was performed.
- Background checks may be performed for cause.
- The results of the background check must be documented and the results reviewed—and the review documented—by the utility per its documented risk assessment program.
- The risk assessments are to be performed in accordance with federal, state, provincial, and local laws and subject to existing collective bargaining agreements.

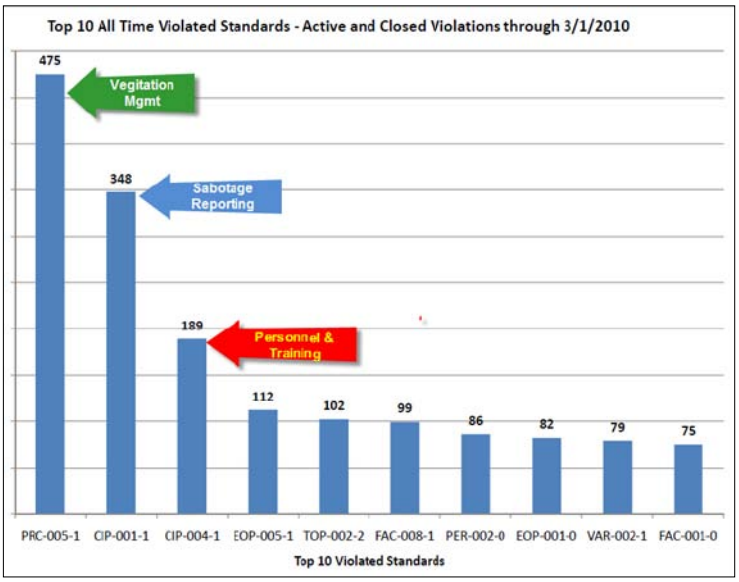
Requirement 4–Access: The affected utility needs to maintain lists of personnel with authorized cyber or authorized unescorted physical access as mandated. These lists need to show the individual's specific electronic and physical access rights to critical cyberassets (e.g., READ, WRITE, DELETE, Physical Adjustment and Repair, etc.)

The lists need to be reviewed quarterly, and the performance of the reviews needs to be documented. Also, the lists need to be updated within seven calendar days of any change to access rights of those personnel listed. Remember, this also includes contractors and vendors as well as employees.

A final key requirement is that the utility shall revoke such access to Critical Cyber Assets within 24 hours (note: not working hours but calendar hours) for personnel terminated for cause (i.e., hostile termination) and within seven calendar days for personnel who no longer require such access (i.e., friendly termination or friendly transfer).

Hardest CIP to enforce

Although the requirements are straightforward, this has been one of the hardest CIP standards for utilities to consistently enforce. In NERC's monthly violation reports, CIP-004 is usually the second most violated reliability standard. In NERC's Top 10 All Time Violated Standards, the March 2010 graph is displayed at right.



Because of the excessive frequency of the violations to CIP-004, in December 2009 NERC produced an analysis of the causes for these compliance failures. The conclusion by NERC first recognized that the violations for CIP-004 generally fell into one of four categories: 1) Documentation, 2) Access (i.e., access without training or clearance), 3) Training, or 4) Risk Assessment (i.e., background check). The number of violations in each category was about the same (20) with risk assessment causing the most failures (24).

Following this analysis, the NERC recommendations to utilities to reduce these violations included ensuring and verifying that employees, contractors and vendors have received training and background checks prior to access and that appropriate changes to access lists are made upon termination or transfer of employees/contractors/vendors.

Vendor guidance and to-do's

For vendors working with electric utilities, it is in your and the utility's best interest to thoroughly understand these requirements and work closely together to ensure the requirements are not only met, but effectively and accurately documented. At the top of the list of things to do, the vendors need to keep the utility informed of any changes to personnel status that could impact the utility access control lists. In other words, if a vendor employee with a utility badge is terminated or resigns, it is of the utmost importance to inform the utility ASAP so they don't miss the 24-hour window for hostile terminations.

Ernie Hayden is the former CISO for the Port of Seattle, Group Health Cooperative and most recently Seattle City Light where he coordinated the efforts regarding NERC Critical Infrastructure Protection compliance. Hayden holds a CISSP and a Certified Ethical Hacker and lives in the Seattle area.

OPINION

Make Critical Infrastructure Protection a Priority

Government and industry leaders need to prioritize CIP in order to preserve the way of life in the United States.

BY JERRY FREESE

THERE'S A MULTIDIMENSIONAL approach to information security in the electric sector. On the business side, we have to protect the corporate networks and data. On the operational side, critical control system security is a mandate from industry groups and regulators. Given the reality of the financial and resource commitments these approaches require, it's often easy to forget that both exist in a larger security context of critical infrastructure protection (CIP).

In today's environment of competing financial requirements, CIP is understandably less a direct driver of security than it is an indirect beneficiary of whatever protection is deemed effective and affordable for business conduct or regulatory compliance. It's not the best situation given that CIP is key to the preservation of the social and economic fabric of our way of life. That would sound like pure melodrama if it weren't so true.

In today's environment of competing financial requirements, CIP is understandably less a direct driver of security than it is an indirect beneficiary of whatever protection is deemed effective and affordable for business conduct or regulatory compliance.

Even so, and in spite of the rhetoric from government and industry groups, the concept of critical infrastructure protection is little more than that…an understated and under-socialized concept, reserved for academics and government planners, lacking any tangible national-level threat to make it a real priority.

What's the reason that a compelling and imperative concept such as critical infrastructure protection hasn't been embraced for its own sake and hasn't prompted actions to ensure its implementation and long term viability? In some respects it comes down to perceived need.

Remember that prior to 2001, the electric sector and critical infrastructure in general enjoyed an essentially threat-free environment. Infrastructure assets and systems were largely isolated from one another, and even damage from natural disasters could be localized without fear of major cascading outages. In other words someone would have to "be here" to conduct attacks against the U.S. infrastructure and the impact

would probably be limited to specific assets and geographic areas.

Now the situation has changed. With the increased use of the Internet and multiple-system connectivity, the electric grid has become an interconnected and complex system of systems, with benefits of speed, efficiency and relatively low cost associated with its control and growth. From the industry perspective, the benefits were a boon for business and unprecedented growth in the use of advanced technology for grid management and communications.

Security professionals are well aware that these changes come with a significant downside. Previously closed and remotely unreachable systems are suddenly vulnerable to a host of Internet-based malicious activities. It takes little imagination to understand that the critical electric infrastructure, so essential to American society, is suddenly at risk of becoming a prime target of hackers, social activists, nation-states and even terrorist organizations, with potentially society-altering consequences.

It takes little imagination to understand that the critical electric infrastructure, so essential to American society, is suddenly at risk of becoming a prime target of hackers, social activists, nation-states and even terrorist organizations, with potentially society-altering consequences.

Government and industry are attempting to address this technology adoption with cybersecurity standards and proposed legislation mandating a more reliable bulk power system. It's a good start, but the first iterations of these standards only apply to a subset of the electric sector assets. Cybersecurity in the electric sector, which typically requires a comprehensive logical protection scheme across all networks and systems, has started to look a lot more like an exercise in specific, major asset compliance than it does an all-encompassing, risk-based, infrastructure protection strategy. Though this approach is more sensitive to financial requirements and considers the sheer scope of the infrastructure, it still suffers from the lack of true commitment to critical infrastructure protection.

What are the missing ingredients? First, it goes back again to perceived need. For most people, the idea of a potential major cyberattack on critical infrastructure, one that could provide the same net effect as actual physical destruction of assets and services across major geographic areas is difficult to grasp. Because we can't see the threat and haven't experienced any real digital warfare or its effects, we don't mobilize nationally across the public and private sectors and prepare our defenses against it. Contrast that with a hypothetical situation where hostile forces are amassed at a U.S. border or a country has deployed a space-based offensive missile system. The national response would be immediate and decisive. The public would demand effective defensive measures be put in place, just in case the forces mobilized or missiles were fired. Protecting the people and the critical infrastructure would be the primary mission.

That brings us to the final missing ingredients; sufficient awareness of the threat and understanding of what we stand to lose in a major cyber incident. There are

numerous individuals and groups throughout the world that are fully capable of launching cyberattacks against our infrastructure. The threat may not be imminent but it can manifest itself very quickly. If we're not actively going to pursue a national (private and public) information campaign and protection strategy, integrating strong security into our essential systems and services, the consequences to our critical infrastructure in the event of an attack could be severe. We need a "just-in-case" mentality for CIP. Our country and our way of life may depend on it.›

Jerry Freese is Director of IT Security Engineer at AEP.

FOREIGN THREATS

Experts Alarmed Over U.S. Electrical Grid Penetration

Foreign probes of the electrical grid has prompted a call on lawmakers to act quickly to strengthen cybersecurity.

BY ROBERT WESTERVELT

THE POTENTIAL for attack on the nation's power grid is fueling alarm in the cybersecurity community, with experts warning that the federal government should act quickly or face the consequences of having the nation's infrastructure crippled by cybercriminals abroad.

"This is the American way of life that is being threatened," said Alan Paller, director of research at the SANS Institute, a Bethesda, Md.-based nonprofit cybersecurity research group. "We need continuous automated monitoring and real oversight of these critical systems and it needs to be a top priority."

Current and former national security officials told *The Wall Street Journal* that malware discovered on electrical grid computer systems suggests that someone abroad could damage the system in a time of war or during a national security crisis in the United States. In addition to the nation's power grid, nuclear power plants and water and sewage systems are also at risk. Financial networks could also be disrupted.

The nation's power grid and other critical infrastructure are connected to networks and systems that have indirect access to the Internet and can be penetrated by attackers.

The nation's power grid and other critical infrastructure are connected to networks and systems that have indirect access to the Internet and can be penetrated by attackers. From there, a sophisticated hacker could make their way into a critical system, Paller said. In February a consortium of federal agencies released a draft of the Consensus Audit Guidelines (CAG), a list of 20 cybersecurity controls that organizations should use to defend against attacks. Paller said power systems should be immediately tested against those 20 critical controls and penetrated computers should be replaced.

"The separation of the power grid from the Internet was part of the design, but in reality there are typically interconnection points," said Ed Skoudis, founder and senior security consultant with InGuardians Inc. Skoudis was the technical editor that helped pull together the CAG list from guidelines issued by the National Institute of Standards and Technology (NIST) and other organizations.

Making matters worse, experts say, is the power grid's mixture of complex legacy systems and aging equipment with different communication protocols. Power companies are investing in modernization, deploying millions of automated metering systems, designed to increase automated command and control of the power grid and reduce the need to send out an agent to physically monitor power consumption. But Skoudis said the systems are not being fully vetted for security by independent testers. The federal stimulus law includes $4 billion in funding that could go toward deploying automated metering systems.

"These smart meters are accessible via wireless and some of them are accessible via the Internet," Skoudis said. "It's just another access point for someone to attack and exploit."

"These smart meters are accessible via wireless and some of them are accessible via the Internet. It's just another access point for someone to attack and exploit."

–ED SKOUDIS, founder and senior security consultant, InGuardians Inc.

One way to respond to the threat is by increasing the powers of the North American Electric Reliability Corporation (NERC), said SAN's Paller. NERC, an organization of U.S. electrical grid operators, oversees standards for the industry. Paller said NERC could be transformed from an industry association into a powerful regulatory body that oversees cyber-security issues and tests energy companies for compliance with a set of standards.

NERC may be a good starting point, said Tim Belcher, chief technology officer of network security monitoring firm NetWitness, which has a number of federal government contracts. Belcher has led assessments of various power and utility supervisory control and data acquisition (SCADA) networks and said he is not surprised that compromises exist.

"We've known that energy command and control networks are valuable targets and are actively being probed," Belcher said. "In general security in those environments has focused on limiting access and not providing security in depth, taking a look inside the network of what can be controlled."

Congress has not been silent on cybersecurity issues of late. Legislation is being debated that creates a cybersecurity advisor in the White House and strengthens cyber-security regulations for the private sector. The proposed legislation would require a complete threat assessment for both government and private systems. Organizations that own pieces of the nation's critical infrastructure would also have to follow federal security standards.

NetWitness' Belcher said the best defense is continued and pervasive monitoring.

"People in the industry are very aware that disconnecting is not an option and they need to focus on perimeter controls, but it's difficult to implement security in-depth because they have very diverse and aging equipment," he said.›

Rob Westervelt is News Director of the Security Media Group at TechTarget.

TECHTARGET SECURITY MEDIA GROUP

SearchSecurity.com

EDITORIAL DIRECTOR Michael S. Mimoso

SEARCHFINANCIALSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS DIRECTOR Robert Westervelt

ASSISTANT EDITOR Maggie Sullivan

ASSOCIATE EDITOR Carolyn Gibney

ASSISTANT EDITOR Greg Smith

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

VICE PRESIDENT/GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Nick Dowd

SALES DIRECTOR Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Allyson Kinch

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Andrew McHugh, Karina Rousseau

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann
peichmann@techtarget.com

Jason Olson jolson@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Jeff Wakely

EUROPEAN DISTRIBUTION
Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336 Fax 781-657-1100

TechTarget
Where Serious Technology Buyers Decide

"Technical Guide on NERC Compliance" is published by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.

SPONSOR RESOURCES

nCircle

See ad page 2

- Whitepaper Download: nCircle Solutions for NERC CIP Compliance
- Whitepaper Download: Configuration Auditing - The Next Critical Step in Compliance
- Whitepaper Download: Five Critical Steps of a Complete Security Risk and Compliance Lifecycle

---

Alert Enterprise, Inc.

See ad page 4

- Protect Critical Assets, NERC CIP Compliance, Validate Traininig and Restrict Physical Access Now!
- AlertEnterprise Selected Gartner 2010 Cool Vendor for Identity and Access Management - read report
- FERC Codes of Conduct - Manage Emlployee Access Rules and Automate Compliance

---