TOP FIVE NERC CIP AUDIT FAILS

FROM THE 2013 NERC CIP RELIABILITY COORDINATOR COMPLIANCE ANALYSIS REPORT

ADVANCED THREAT PROTECTION, SECURITY AND COMPLIANCE

EXECUTIVE SUMMARY

Protecting our Critical Infrastructure has been an increasing cybersecurity concern from our nation's highest office on down. The US (and some Canadian provinces') power and electric industry has been subject to the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Cyber Security Standards since 2008, and the February 12, 2013, Presidential Policy Directive 21 (PPD 21) named the Energy Sector as one of its 16 named Critical Infrastructure Sectors subject to its security standards.

NERC's CIP standards are essentially minimums, and while major strides have been made in setting and upgrading compliance standards by the US Federal Energy Regulatory Commission (FERC) and NERC in these past six years, it's clear there is much more that must be done—and with a much higher sense of urgency.

This white paper examines the five most violated NERC CIP compliance audit findings from NERC's 2013 *Reliability Coordinator Compliance Analysis Report* in an effort to underscore key findings and urgent takeaways for all affected businesses. It also examines the latest Government Accountability Office (GAO) guidance as to why audit findings are often ignored.

◆ "While no unclassified reports have been published regarding a terrorist-initiated cyber-attack on U.S. critical infrastructure, the vulnerability of essential components of that infrastructure to access and even destruction via the Internet has been demonstrated." ◆

THE 2013 CYBERSECURITY EXECUTIVE ORDER: OVERVIEW AND CONSIDERATIONS FOR CONGRESS

INTRODUCTION

The "Northeast Blackout of 2003" was the largest power outage in US history, leaving more than 50 million people without electricity for up to an entire day beginning after 4pm (EDT) on August 14th, 2003. This outage cost approximately $6 billion, led to 11 deaths (fewer than might be expected by such an event) and left millions of homes and businesses across the US Midwest, Northeast, and Ontario Canada without electricity.

Initially, public perception of the cause for this outage was highly focused on the possibility it was a new incidence of terrorism, since 9/11 was less than years prior. The eventual explanation was that it was the culmination of a cascading series of events, including a software bug in an alarm system, trees on power lines and a spike in energy usage due to a heat wave.

Certainly the experience for those affected was a foretaste of what attackers could do to the power grid. Six years later, "(i)n 2009, the Department of Homeland Security conducted an experiment that revealed some of the vulnerabilities to the nation's control systems that manage power generators and grids. The experiment, known as the Aurora Project, entailed a computer-based attack on a power generator's control system that caused operations to cease and the equipment to be destroyed," (from "*Challenges Remain in DHS' Efforts to Secure Control Systems*," Department of Homeland Security, Office of Inspector General, August 2009).

The energy sector is one of 16 named as Critical Infrastructure in the February 12, 2013 PPD 21. As demonstrated in 2003, electricity is an asset essential for US society and economy to function (a working definition of critical infrastructure), and examining NERC reports on common violations have implications which should be urgent for all of us.

THE TOP FIVE MOST VIOLATED CIP STANDARDS

The power and electric industry has one underlying mission: the reliable delivery of electricity. Many in the industry see audit requirements such as NERC CIP standards to be a major distraction from their core mission. Nevertheless, the industry is mandated to comply or face serious financial costs—fines and penalties totalling nearly $160 million have been levied in the past five years, according to sources at NERC.

The NERC May 2013 Reliability Coordinator Compliance Analysis Report summarizes 140 total CIP violations since 2008 (when compliance with CIP-002 through CIP-009 became mandatory). Compared to a total of 58 Operations & Procedures recorded violations (ten in the past two years), clearly CIP violations are the majority of all reported violations.

Despite improved compliance trends, especially in self-identified violations within the power and electric industry, these five CIP standards continue to challenge Registered Entities:

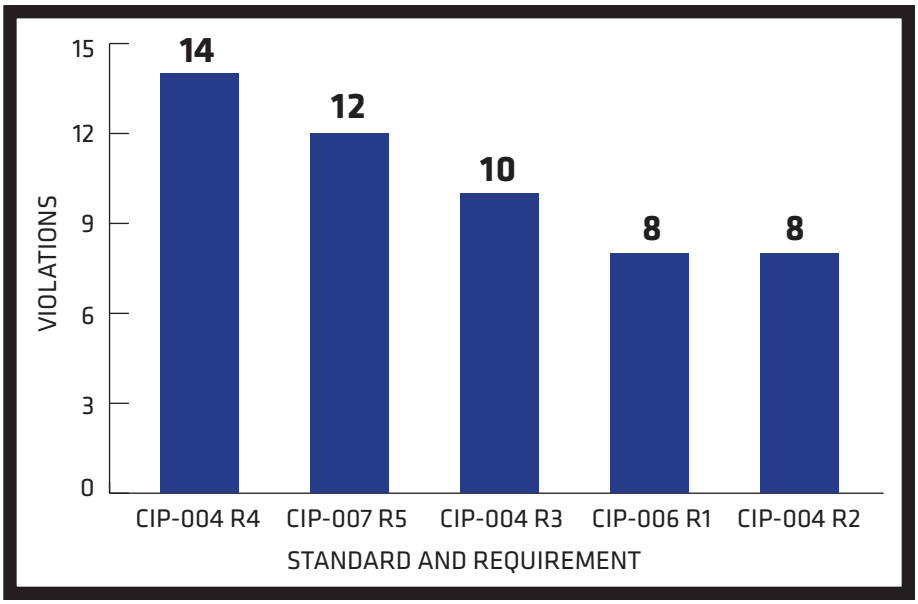
- CIP-007 – Systems Security Management
- CIP-004 – Personnel and Training
- CIP-005 – Electronic Security Perimeter(s)
- CIP-006 – Physical Security of Cyber Assets
- CIP-003 – Security Management Controls

TOP CIP RELIABILITY COORDINATOR VIOLATIONS

All-Time		January 1, 2011–December 1, 2012	
Standard	**Violations**	**Standard**	**Violations**
CIP-007	52	CIP-004	6
CIP-004	32	CIP-007	5
CIP-005	16	CIP-003	3
CIP-006	15	CIP-006	2
CIP-003	12	CIP-005	2

◆ As reported on in the NERC Reliability Coordinator Compliance Analysis Report, May 20, 2013

TOP 5 RELIABILITY COORDINATOR CIP VIOLATIONS BY REQUIREMENT (ALL-TIME)



DETAILED VIOLATION INFORMATION BY STANDARD AND REQUIREMENT

CIP-004 – PERSONNEL AND TRAINING

REQUIREMENT 4 – ACCESS

Requires entities maintain a list of personnel who have authorized cyber or unescorted physical access to Critical Cyber Assets. This list must be reviewed at least every quarter and updated within seven calendar days of any change in access rights of personnel or change of personnel with access to Critical Cyber Assets. Further, in the event an employee is terminated, the entity must revoke the employee's access to these assets within 24 hours.

Notable Violation Examples

- Failed to maintain a list of personnel with authorized access.
- Failed to revoke cyber access to Critical Cyber Assets for two employees within seven days after the employees retired.
- Entity could not provide evidence that they maintained lists of personnel's specific electronic and physical access rights to Critical Cyber Assets.
- Entity granted personnel unescorted, physical access (using temporary access cards) without properly documented authorization.
- Failed to maintain, review, and update access lists containing detailed access rights of personnel with authorized cyber or unescorted, physical access to Critical Cyber Assets for a portion of the audit period.
- Vendor access lists for EMS and SCADA systems reviewed annually, not quarterly.

Suggested Mitigations and Takeaways—Additional security measures, procedures, and quarterly reviews.

- Entities should consider adding additional security measures such as key card access, security guards, and video monitoring in order to prevent unauthorized access to Critical Cyber Assets.
- Better procedures for updating lists when user access changes or employee is terminated.
- Quarterly, not annual reviews of authorized user access lists.

CIP-007 – SYSTEMS SECURITY MANAGEMENT

REQUIREMENT 5 – ACCOUNT MANAGEMENT

Requires entities to establish, implement, and document technical and procedural controls that enforce access authentication of—and accountability for—all user activity, and that minimize the risk of unauthorized system access. These controls ensure user permissions are consistent with need-to-know information and prevent shared access of user accounts that do not have audit trails.

Notable Violation Examples

- Five terminal servers in the Electronic Security Perimeter did not have implemented and documented technical and procedural controls and accountability to enforce access authentication, accountability for all user activity, and minimized risk of unauthorized system access.
- Password criteria were not defined in CIP policy as requiring the three CIP-specific characters (alpha, numeric, special).
- The local Windows password age was 1706 days (not changed in 4.5 years) at the time of discovery.
- The factory default accounts for cyber assets were not changed prior to putting the devices into service. These cyber assets were used in access control and monitoring of the Physical Security Perimeter, providing authorization and log access. The passwords were last changed in March of 2010. There was also no policy implementation to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges (including factory default accounts).

Suggested Mitigations and Takeaways—Need-to-know and password hygiene.

- Need-to-know basis for personnel access to Critical Cyber Assets. Suggestions are to create and maintain a list of personnel with system access, documenting access each has.
- Implement software that enforces user passwords to Critical Cyber Assets be changed annually. (This is from the NERC report, but common organization goals will have a 90-day or less password age.)
- Review and confirm that passwords are changed.
- Avoid joint accounts that allow multiple users access to the system under one user name and password.
- Institute an audit trail to document all individuals with access to the account if joint accounts must be used.
- Technical Feasibility Exception (TFE) requests should be submitted when potential gaps are required due to equipment limitation.

CIP-004 – PERSONNEL AND TRAINING

REQUIREMENT 3 – PERSONNEL RISK ASSESSMENT

Requirement mandates entities have a documented personnel risk assessment program for personnel with authorized cyber or unescorted, physical access to Critical Cyber Assets. Personnel risk assessments must be updated at least every seven years.

Notable Violation Examples

- Failed to demonstrate that personnel risk assessments had been received by all personnel with logical or physical access to Critical Cyber Assets.
- Background checks did not meet the time span required, though the entity

had background check procedures in place.

- An employee was granted physical access to a protected area without prior documentation of a personnel risk assessment.
- Four individuals were granted access without conducting the required assessment within thirty days of being granted access as documented by its personnel risk assessment program.
- Failed to ensure that each personnel risk assessment include identity verification, and a seven-year criminal check. Also failed to update each personnel risk assessment every seven years.

Suggested Mitigations and Takeaways—New hire training, access procedures, and access lists maintained by Compliance.

- Revoke Critical Cyber Asset access for individuals who do not have an up-to-date personnel risk assessment completed.
- Consolidate access lists into one list to be maintained by the compliance department.
- Establish procedures that mandate employees complete personnel risk assessments as part of their new hire training.

CIP-006 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

REQUIREMENT 1 – PHYSICAL SECURITY PLAN

Requires that entities maintain, implement, and document a physical security plan that is approved by the senior manager. Violations of this requirement have occurred for a variety of reasons including failure to maintain a six-wall perimeter, identify all physical access points, and escort visitors at all times.

Notable Violation Examples

- Not all in-scope, identified physical security perimeters incorporated a completely enclosed (six-wall) border.
- Failed to create and maintain a physical security plan that was approved by a senior manager.
- Failed to provide all the protections specified for Cyber Assets that authorize and log access to the physical security perimeter.
- Failed to provide continuous escorted access of visitors within the physical security perimeter.
- Failed to ensure the appropriate use of physical access controls at one access point to one physical security perimeter.
- Incorrect implementation of its physical security plan due to the unavailability of the plan.

Suggested Mitigations and Takeaways—Reminders, Signage, and Additional Training.

- Develop a mitigation plan that distributed reminders of procedures required for all personnel to follow when escorting visitors.
- Installation of clearly visible door signs at each applicable access door reminding employees to be aware of individuals behind them when entering secure areas.
- Requiring all corporate IT personnel to complete the entity's cyber security training program.

CIP-004 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

REQUIREMENT 2 – TRAINING

Requires entities to establish, document, implement and maintain an annual cyber-security training program for personnel with authorized cyber or unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually at a minimum, and shall be updated whenever necessary.

Notable Violation Examples

- The entity's 2009 training material did not address acceptable use of Critical Cyber Assets.
- Failed to provide sufficient evidence that five contractor employees had completed cyber security training within 90 days of being granted access to Critical Cyber Assets.
- Some employees had not completed the company training for access, yet had physical access to Critical Cyber Assets.
- Failed to provide evidence that security training was completed for employees who had unescorted access to Critical Cyber Assets.
- Failure to provide evidence of training within 90 calendar days for all personnel with authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors.

Suggested Mitigations and Takeaways—Reminders, Signage, and Additional Training.

- Purchasing standards compliance tracking software application that automatically sends an email notification to all personnel with authorized access to Critical Cyber Assets reminding them to complete the required training.

SUMMARY

Data breaches and the evolving threat landscape are in global news nearly every day. Insights from investigating these very public breaches indicate that attackers were often at work long before the companies detected their presence. Forensics in some cases indicate hiding "in plain sight" by using valid credentials, application user IDs and even storing stolen information from within the target company's infrastructure. Breaches and exfiltration can take only minutes—and discovery months to years.

In the internet security field, none of this is news. However, when critical infrastructure is at risk due to themes of week password hygiene, poor physical and cyber access controls and a lack of good training and awareness, urgency is due.

Jeffrey Wilshusen is the director of information security issues at the US Government Accountability Office, and often issues advice to agencies to improve their security. He'll admit that his recommendations are not always heeded. He notes the that rapid pace of change in both technology and business processes places strain on IT security to protect and manage data in environments burdened with inherent risk. Portable devices, third party operators, and shared systems only add more.

Attackers are agile and the threats are constantly changing—faster than defenders can keep up. The recent 2014 Verizon *Data Breach Investigations Report* showed that attackers can sometimes successfully breach in minutes, while it may take defenders days, months and even before they can detect the breach, if they ever do. All too often its a third party, customers or users make the discovery.

Finally, emphasizing mission over security could explain why many organizations often can fail to take auditor's advice to strengthen security controls. Doesn't this sound all too familiar?

TRIPWIRE COVERAGE OF NERC CIPv5 REQUIREMENTS

10 Standards | 32 Requirements | Tripwire covers 20

CIP-002 BES CYBER SYSTEM IDENTIFICATION AND CATEGORIZATION	CIP-003 SECURITY MANAGEMENT CONTROLS	CIP-004 TRAINING AND PERSONNEL SECURITY	CIP-005 ELECTRONIC SECURITY PERIMETER	CIP-006 PHYSICAL SECURITY OF BES CYBER SYSTEMS	CIP-007 SYSTEMS SECURITY MANAGEMENT	CIP-008 INCIDENT REPORTING AND RESPONSE PLANNING	CIP-009 RECOVERY PLANS FOR BES CYBER SYSTEMS	CIP-010 CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENTS	CIP-011 INFORMATION PROTECTION
1. BES CYBER SYSTEM IDENTIFICATION	1. CYBER SECURITY POLICY FOR HIGH/MEDIUM SYSTEMS	1. AWARENESS	1. ELECTRONIC SECURITY PERIMETER	1. PHYSICAL SECURITY PLAN	1. PORTS AND SERVICES	1. CYBER SECURITY INCIDENT RESPONSE PLAN	1. RECOVERY PLAN SPECIFICATIONS	1. CONFIGURATION CHANGE MANAGEMENT	1. INFORMATION PROTECTION
2. REGULAR APPROVAL	2. CYBER SECURITY POLICY FOR LOW SYSTEMS	2. TRAINING	2. INTERACTIVE REMOTE ACCESS MANAGEMENT	2. VISITOR CONTROL PROGRAM	2. SECURITY PATCH MANAGEMENT	2. CYBER SECURITY INCIDENT RESPONSE PLAN IMPLEMENTATION AND TESTING	2. RECOVERY PLAN IMPLEMENTATION AND TESTING	2. CONFIGURATION MONITORING	2. BES CYBER ASSET REUSE AND DISPOSAL
	3. IDENTIFICATION OF SENIOR MANAGER	3. PERSONNEL RISK ASSESSMENT PROGRAM		3. MAINTENANCE AND TESTING PROGRAM	3. MALICIOUS CODE PREVENTION	3. CYBER SECURITY INCIDENT RESPONSE PLAN REVIEW, UPDATE, COMMUNICATION	3. RECOVERY PLAN REVIEW, UPDATE AND COMMUNICATION	3. VULNERABILITY ASSESSMENTS	
	4. DELEGATION OF AUTHORITY	4. ACCESS MANAGEMENT PROGRAM			4. SECURITY EVENT MONITORING				
		5. ACCESS REVOCATION PROGRAM			5. SYSTEM ACCESS CONTROLS				

◆ Tripwire is a leading provider of advanced threat, security and compliance solutions that enable enterprises, service providers and government agencies to confidently detect, prevent and respond to cybersecurity threats. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business-context, and enable security automation through enterprise integration. Tripwire's portfolio of enterprise-class security solutions includes configuration and policy management, file integrity monitoring, vulnerability management and log intelligence. Learn more at tripwire.com. ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

WPCIPAF1b 201404