KPMG

Plugged In

Issues impacting the power and utilities industry

Checking in on the utility industry's compliance with NERC CIP standards.

In this edition of the Global Energy Institute's *Plugged In*, we asked Michael Gomez and Tim Johnson from KPMG LLP's (KPMG) Cyber Security Services for an update on the progress utilities are making in complying with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) plan.

1. **NERC CIP versions 5 and 6 brought big changes to the electric utility space. What are the key takeaways from the first year of operations under these updated requirements?**
   Since July 2016, most utilities focused their NERC CIP v5/v6 programs on performing a large-scale introduction of new technologies and controls to their operational environments. However, they were challenged with a relatively short implementation period, multiple tech deliveries happening in parallel, and incomplete deliveries requiring manual workarounds to achieve the desired functionality. Since then, utilities have been struggling to figure out what is actually in place, where the gaps lie, and what is not working as planned.

   To further complicate matters, utilities had to contend with business units such as power generation stations that have been run independently for years. Add to the mix a number of acquisitions by many of the larger companies and a traditionally decentralized approach to compliance, and to date many utilities have struggled—and failed—at achieving the required enterprise-wide compliance with the updated standards.

2. **As utilities prepare for the first round of compliance audits, where are they focusing much of their effort?**
   In two areas: operationalizing NERC CIP by making sure new tools and methods are properly functioning and in use; and evidence management for data-driven proof of compliance.

   While the utilities had 18-plus months to prepare for NERC CIP v5/v6, they had to be operating compliantly by the middle of 2016 or face potential violations and fines. Unlike other security standards where the management of acceptable risk is the objective, NERC CIP focuses on strict compliance. You either "are" or "are not."

Welcome to KPMG Global Energy Institute's *Plugged In*. Specialists address key issues in the power and utilities sector. *Plugged In* offers insight from KPMG thought leaders on the trends that are driving and shaping power and utility companies today.

Michael Gomez
Principal, Advisory
Cyber Security Services
KPMG LLP (U.S.)

Tim Johnson
Manager, Advisory
Cyber Security Services
KPMG LLP (U.S.)

About the GEI

The KPMG Global Energy Institute (GEI) is a worldwide knowledge-sharing forum on current and emerging industry issues. Launched in 2007, the GEI interacts with its over 30,000 members through multiple media channels, including audio and video Webcasts, publications and white papers, podcasts, events, and quarterly newsletters. To become a member, visit www.kpmgglobalenergyinstitute.com.

Utilities now have some experience using (or unfortunately in many cases, not using) their new tools and processes. Debates about organizational and individual roles and responsibilities continue. Initial assessments of evidence artifacts have come back as incomplete or inaccurate. Lessons are being learned, while at the same time, operational and maintenance costs are creeping up as manual tasks persist and even more workarounds are put in place.

During this shake-out period, utilities are facing an increased volume of potential violations and self-reports as their performance proficiency lags and the new the reporting thresholds are more finely calibrated.

3. What is the next stage for NERC CIP requirements?

Draft standards for supply chain management (CIP-013) as well as v5/v6 cleanups are well underway, and the Federal Energy Regulatory Commission (FERC) is applying pressure on NERC to have these updates in place within the next year.

CIP-013 will not only require utilities to step up their vendor management game, but also require the vendors themselves to change the way they work and support their products. Utilities may also seek to pass along potential NERC CIP violation liability to their suppliers, if the suppliers provide defective materials, information, or support. A vendor's ability to support the updated supply chain management process will potentially become a differentiator in the market.

4. Why is complying with NERC CIP so challenging?

The standard answer is, "it's complicated." While NERC CIP is complex and imperfect, at its core it is rather simple and can be summarized in a few key points:

- *Know your mandatory baseline items for protected cyber assets.* What do you have installed, where, and how is it configured?
- *Control how your baseline changes over time.* Capture patches, upgrades, swap outs, etc., and make sure a responsible party knows about the changes.
- *Limit access.* Make sure that anyone who accesses the baseline is known, authorized, and only able to perform tasks they are assigned and approved to do.
- *Alert and respond.* Monitor the baseline physically and electronically. If something is outside the norm, do not ignore it—check it out.

And yet, compliance with NERC CIP is hard because despite all of the technology and automation, most of the impactful controls and protections rely on people. Unfortunately, the industry has done a poor job identifying the specific slice of work each employee needs to do, do well, and do consistently to help ensure compliant and reliable operations.

Where utilities consistently fall down is not following through on organizational change management all the way down to the individual operators who need to adjust how they do their jobs to act in a NERC CIP-compliant manner.

5. How have additional requirements for low-impact facilities, transient cyber assets, and removable media affected utilities?

These requirements have added twists to utility compliance programs.

Utilities have underestimated or overlooked the requirements for low-impact facilities as they tackled the more extensive and early enforceable standards for high and medium assets. On the surface, the requirements seem minimal, like a subset of the existing requirements. Maintaining a list of low-impact cyber systems is not explicitly required.

However, most utilities have come to realize that such a list is needed from a practical point of view, even if the list itself is not subject to audit. The effort requires some improved change management processes to at least identify when equipment is moved, added, or subtracted.

The requirements for transient cyber assets and removable media cut across the practical implications of allowing temporary connections to a secure environment without impacting security. To be successful, enhanced change controls are needed along with pre- and post-connect screening and clear authorization for the connection. Evidence supporting all aspects of the transactional connection have to be captured, reviewed, and maintained. Since many of these connections occur in the field, the impact is on employees who are not typically accustomed to such rigor when their primary duty is to restore service as soon as possible.

6. What are the security implications for the utility of the future?

We can imagine the emerging energy landscape and utility of the future will include any number of elements, from connectivity between third-party suppliers, a smart grid, and industrial-scale power storage to tighter coupling between real-time energy demand and energy production, more competitive markets—even utilities taking on a role as another "flavor" of Internet or entertainment service provider.

But the one thing all of these visions have in common is exponential growth in data and information from a wide spectrum of sources—customer, operational, supplier, market, service, etc. These sources will need to be smartly integrated to deliver real value, but the integration also needs to address security and privacy across competing statutes, regulations, and jurisdictions.

Consider how a bad actor could manipulate smart grid data to project a fictitious spike in demand, and then benefit financially from the artificial market pricing.

As utilities increasingly become data and command hubs not only for electricity but also for other services and streams, they will be forced to adopt a thorough approach to operational security and privacy spanning the traditional stovepipes of IT, OT, business, corporate, and finance.

Contact us

Michael Gomez
Principal, Advisory
T: 202-533-5007
E: michaelgomez@kpmg.com

Rangana Guha
Director, Advisory
T: 617-988-1347
E: rguha@kpmg.com

Tim Johnson
Manager, Advisory
T: 214-840-4449
E: timjohnson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia