UpGuard™

WHITEPAPER

Understanding NERC and Picking a Compliance Solution

ABOUT THIS WHITEPAPER

Compliance with **NERC CIP** standards is both important and complex. This whitepaper explains what the North American Electric Reliability Corporation (NERC) is, how it came about, what challenges Critical Infrastructure Protection (CIP) compliance introduces for companies and how to get the most value from a NERC compliance solution. This whitepaper is for both technical and non-technical people interested in NERC standards or responsible for NERC compliance within their organization.

ORIGINS OF NERC

In 1965, over 30 million people lost power in **an enormous power blackout** lasting 13 hours. It turned out that a relatively minor error made in Ontario cascaded across the interconnect and overloaded most of the lines. This event spurred the electric utility industry to create NERC, (then the North American Electric Reliability Council) which formalized planning guides and operating procedures to prevent this kind of large scale outage from happening again.

As isolated power stations began linking up through interconnects, creating the huge grids we know today, the danger of a single event impacting the system increased both in likelihood and consequence. An **electric interconnect**, also known as a synchronous grid, allows multiple power generation sources to pool in a single zone with a synchronized frequency. In normal operating conditions, the interconnect improves overall efficiency, but the nature of the synchronous grid allows for the cascading of one problem across the zone. NERC regulates certain key procedures and protocols to prevent the most likely incidents from occurring at all, by ensuring that companies abide by a set of standards.

But in 2003, **yet another blackout** hit the northeast, this one even worse than the 1965 incident, affecting 55 million people, including a dozen fatalities, with recovery times ranging from hours to weeks. The **following investigations found** that the FirstEnergy (FE) corporation in Ohio had neglected their regulations, citing that they “failed to assess and understand the inadequacies of their system” and “did not recognize or understand its deteriorating condition.”

What set this incident apart was that the primary cause was a computer software bug that took down FirstEnergy’s alarm system for over an hour. During this period, FE was flying blind, unaware of alerts or changes in the system, and a single power station in Ohio going down was enough to push the entire electrical load onto high power lines, which came in contact with overgrown trees, shutting down over 100 power stations.

Like the 1965 incident, the 2003 outage was representative of the risk interconnected systems face, but unlike the previous outage, this one only happened because FirstEnergy lost visibility into their computer environment and were unable to utilize the tools and measures created to handle incidents such as the downed power station and overgrown tree contact. It was clear that IT computer systems were every bit as critical to the interconnected infrastructure as the power stations, perhaps even more so, because while a single power station can fail without taking down the whole grid, a computer failure can affect the whole system, because by design it is intended to centralize the administration of distributed operations.

ORIGINS OF NERC

In recent years, cyber attacks on infrastructure abroad have increased. In December of 2015, hackers were able to shut down part of Ukraine's power grid, affecting 230,000 people. This hack of a German steel mill in 2014 was able to cause actual physical damage, just by changing the configuration settings on a server, and hackers were able to blow up a BP oil pipeline by "injecting malicious software into the control network." Japan's infrastructure, including electric, natural gas and transportation, have been under a continual, likely state-sponsored, cyber attack dubbed "Operation Dust Storm" for years. The counter-terror chief of the European Union warns that nuclear power plants in Belgium face the threat of a cyber attack. It's hardly difficult to imagine computer based attacks, given the physical violence of state conflicts.

Obviously, these attacks abroad are the proof-of-concept that American infrastructure is equally vulnerable to cyber attacks without sufficient protection, and this is why NERC, especially the newer version 5 and the upcoming version 6, focus on cyber security as a critical piece. A 2014 Forbes article outlines how and why America's infrastructure is vulnerable to cyber attacks, stating "the same connectivity that managers use to collect data and control devices allows cyber attackers to get into control system networks to steal sensitive information, disrupt processes, and cause damage to equipment." As early as 2009 NERC was warning that the electrical grid was not properly protected against cyber attacks.

HISTORY AND CHALLENGES OF NERC IMPLEMENTATION

NERC's CIP requirements took effect in 2006, with auditing for compliance beginning in 2007. "One million dollars per day, per violation" was the catchphrase spurring companies into action, who weighed the cost of implementing the NERC regulations against the fines. But the actual fines varied greatly, and although the "million a day" bogeyman persists, enforcement of NERC standards has been difficult. But while fines were relatively weak in the past, there is evidence they have increased this year, and that NERC is starting to put your money where their mouth is.

The different versions of NERC CIPs have also made compliance an ongoing struggle for organizations, or to phrase that differently, the evolution of cyber threats and the resulting security to protect against them have forced NERC to add new requirements and modify old ones. The mandatory compliance with NERC regulations thus brought a previously unnecessary expense into many businesses who are reluctant to accept it as normal operating cost.

Additionally, compliance doesn't always necessarily mean an increase in security. To avoid things that fell within NERC's scope, companies did everything from cancelling otherwise useful security exercises to replacing newer infrastructure with older pieces excluded from NERC's domain.This reverse effect happens because the financial toll of compliance with NERC outweighed other options, such as downgrading infrastructure or simply paying the fines without the intent to correct the problem. If the fines aren't strong enough to drive behavior, they tend to have the effect of merely subtracting from what budget is allocated to security.

Financial considerations weren't the only factor impacting NERC compliance. It takes significant, skilled labor to implement the required safeguards and establish a system of record by which to prove the safeguards are in place. This can lead to the best and brightest documenting the state rather than improving and securing it, undermining the entire effort. The technical and logistical complexity of the NERC standards has also led to persistent misunderstandings, putting the cart before the horse, emphasizing the documentation of the standard rather than the execution of actual security measures.

VERSION 5 AND BEYOND

The NERC CIP Standards version 5 has new sections, including one on change management. This will put companies even further behind in compliance, adding a whole separate level of complexity to the auditing process to verify change management protocols follow standards. For many businesses struggling with simply implementing a change management process in the first place, this will place additional burden on their team to work the documentation effort into the mix, while established change management processes may need to be altered to be brought in line with the new guidelines and to facilitate the required documentation.

In addition to these new sections, old standards must be mapped to the new standards and companies will be expected to address the new CIP requirements in their compliance reports, part of the ongoing overhead of an adaptive standards system. As if that weren't enough, version 6 is just around the corner, with enforcement coming within the next two years. A NERC compliance solution must account for this ongoing change to allow businesses to move with enough agility to stay on top of the requirements.

MAKING NERC WORTH DOING

Ironically, it's easy to lose sight of what's at stake here, given the complexity of the standard and its enforcement. But there are real threats to infrastructure and the NERC guidelines ultimately exist to protect people as much as possible in the event of an incident. Electricity and other public infrastructure are crucial to society. The complexity of the standard speaks to the dedication of people who work to protect these services from the many threats they face. Taking these threats seriously up front and building systems to withstand them will ultimately be less costly than getting hit unexpectedly with a major event resulting in a data breach, outage, or as we've seen is possible, actual physical damage.

Focusing on tools and processes that actually improve systems management and security, as well as people with the correct skillsets to understand and manage them, rather than just reporting the state of compliance, can cut the overall cost of compliance by standardizing systems and testing configurations above and beyond what is required by a standard like NERC. We saw in the example of the 2003 blackout how a lack of visibility into their computing systems rendered them vulnerable to even the simplest of problems. Likewise, increasing visibility into the data center and running existing configurations against policies that check compliance to both standards like NERC and company expectations will proactively head-off many of the attacks and unplanned outages against which the NERC standards are designed to protect.

A properly configured, secured and tested environment not only makes compliance easier and less costly, but can reduce costs and administrative overhead across the board. As prices for insurance against cyber attacks becomes more data driven, based on the existing and historical security state of a particular company, costs here too will be more offset by running an environment that is less at risk.

PICKING A NERC COMPLIANCE SOLUTION

Does it satisfy CIP requirements?	Most importantly, the solution must demonstrate compliance to NERC standards in an audit.
Price	Avoiding fines is the government's "stick" to drive compliance. For better or worse, financial controllers must compare the cost of a solution to the cost of fines, which has led some companies to choose non-compliance as the less costly result.
Deployment Time	A solution that takes months to deploy incurs additional costs in employee time, reduces the amortized value of the solution, and doesn't mitigate the risk of failing audit in the interim. Like pulling off a band-aid, compliance hurts less if it can be done quickly.
Total Cost of Ownership	Beyond the sticker price and the time spent deploying a solution, what's being signed up for down the road? How will the maintenance costs of the solution affect the ability to execute on other projects? And if using the software on day one isn't enjoyable, just imagine after a year or two of steady use. Will it be an albatross? Outdated and complex solutions require specialist knowledge that is increasingly more difficult to come by.
Strategic benefits	You want to pass your NERC audit, but you also want to be good at your job. Consider whether solutions will integrate with other tools and processes, and what benefits they might offer beyond checking the box on compliance. Getting budget for tools that demonstrate compliance is easier than doing so for tools that increase efficiency, but here that's an advantage if the solution can do both.

CONCLUSION

Understanding the history of NERC helps to understand the organic process by which individual, isolated systems began to grow and interconnect, creating an environment where a single incident could have drastic consequences. By regulating the pieces involved in preventing these incidents, NERC attempts to keep crucial infrastructure secure and operable. However, the reality of NERC implementation is less simple, with the documentation of compliance often overshadowing the actual security measures themselves.

SOURCES

http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

https://en.wikipedia.org/wiki/Northeast_blackout_of_1965

https://en.wikipedia.org/wiki/Wide_area_synchronous_grid

https://en.wikipedia.org/wiki/Northeast_blackout_of_2003

https://en.wikipedia.org/wiki/Northeast_blackout_of_2003#Findings

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

http://www.zdnet.com/article/japans-critical-infrastructure-under-escalating-cyber-attack-says-report/

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

http://www.bloomberg.com/news/2014-12-10/the-map-that-shows-why-a-pipeline-explosion-in-turkey-matters-to-the-u-s-.html

http://www.zdnet.com/article/japans-critical-infrastructure-under-escalating-cyber-attack-says-report/

http://www.securityweek.com/belgiums-nuclear-plants-face-threat-cyber-attack-eu-counter-terror-chief

http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/#58f30d86b8aa

http://online.wsj.com/public/resources/documents/CIP-002-Identification-Letter-040609.pdf

http://www.infosecisland.com/blogview/24249-The-NERC-CIPs-Are-Not-Making-the-Grid-More-Secure-or-Reliable.html

https://www.sans.org/media/critical-security-controls/nerc-cip-mapping-sans20-csc.pdf

https://www.ciptraining.org/ferc-approves-nerc-cip-version-6/