

NERC CIP Compliance - Questions the Board Should Ask

Paul J. Feldman and Shelley A. Longmuir

A Board of Directors is charged with oversight of company activities. To accomplish that mission, the Board must take an active role in deciding how it wishes to fulfill that responsibility. This paper presents yet another consideration for Energy Companies' Boards – the proper involvement in a company's responsibility to meet North American Electric Reliability Corporation (NERC) Reliability Standards for the Bulk Electric Systems (BES) of North America (NERC Standards), and Critical Infrastructure Protection (CIP) Standards in particular.

The term 'Compliance' generally refers to ensuring that company personnel are aware of applicable laws and regulations and take appropriate steps to comply. Compliance is a growing phenomenon in corporate America. Energy Companies in particular are exposed to a growing and complex set of requirements. These include the Sarbanes-Oxley (SOX) Act of 2002 (accuracy of financial statements), the Federal Trade Commission's (FTC's) "Red Flags" Rules which go into effect August 1, 2009 to protect customers against identity theft, new and growing NERC Standards (<http://www.nerc.com/page.php?cid=2|20>) related to protecting the BES, and many others.

SOX

The short history of SOX (Sarbanes-Oxley) implementation may help to inform what we can expect as the NERC Standards are implemented. Early in the SOX process, Management and the Board were confronted with a series of requirements and penalties for non-compliance. The rules looked onerous in that they required lots of work and involved substantive penalties, corporate risk, and change. Virtually every company had to make changes to their operations – operations that had been previously developed and optimized. In addition to implementing the required changes to operations – proving the business is compliant is an incremental business function and cost. Changes affected both the Board of Directors and a high percentage of the work force. There was resistance to the required changes from many sources. Various proactive and reactive strategies for dealing with the compliance challenge emerged. In some cases, the compliance discussion even led to reexamination of company values and culture.

Today, just a few years later, there are still SOX proponents and detractors – but the compliance debate has for the most part quieted. Certainly there are Directors that continue to believe that the rules are inappropriate and a burden on the company. However, there are also those that feel a sense of involvement and relief as a result of the increased Management/Board interaction required to assure financial statement accuracy. The roles and responsibilities of both Management and the Board are developed within each company based on law, tradition, Board discussion and negotiation. The dividing line

between Management and the Board is an important debate and decision – and one that evolves based on changing circumstances. The company's Internal Auditors may now report to the Board Audit Committee. Chief Compliance Officer may have a direct responsibility to, or even report to a Committee of the Board. The Chief Risk Officer may also fall into that category. These are all changes that have largely occurred in the last decade.

NERC

The NERC Standards are promulgated to protect the reliability of the BES. They serve to guard against cascading power failures of the type experienced in 1965 (25 million people affected) and in 2003 (55 million people).

Large scale grid operators manage the fleet of generators and transmission lines so as to maintain the reliability of the BES. To prevent against cascading power failures, reserves are carried in real time to allow the grid to continue functioning when any one generator or transmission line fails (N-1 failure protection – read as "N minus 1"). Accomplishment of this feat is no small task in an industry where use of electricity (customer demand, load) and supply must be simultaneously matched to maintain the network. This system works well because N-1 failures are rare - being mother-nature and equipment failure related. Most of the NERC Standards are designed to protect against failures related to these traditional business conditions. Multiple (N-x) failures can occur, however, at a lower probability. To design a system to withstand multiple, simultaneous failures quickly becomes both mathematically and cost prohibitive.

In this current chapter in the energy industry's evolution, the potentially devastating threat of cyber attack has become a reality. On July 5, 2009, there was a wide spread cyber attack on the U.S. Government – comprising attacks on more than 10 agencies and the White House systems. Cyber attacks are not related to mother-nature or equipment failures (traditional N-1 grid management). Cyber attacks are unique for the power grid because they potentially expose the network to large scale simultaneous attacks. Multiple (N-x) failures are the attacker's desired outcome of a concerted simultaneous asset cyber attack and must be defended against using a "Defense in Depth" strategy - protecting assets at the edges of the network as well as at the core (ISOs and other system operators). Michael Assante is the Chief Security Officer for NERC, and in a April 7, 2009 letter (<http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf>) he makes this point and pleads with industry members to be diligent about identification of exposed assets (as part of the BES and potentially related to cascading power failures).

CIP

Presidential (US) directive PDD-63 of May 1998 set up a national program of "Critical Infrastructure Protection" (CIP). The Bulk Electric System is part of the critical national infrastructure. The NERC CIP Standards relate to the national effort, and the traditional efforts of energy companies to protect assets from cascading large scale failures.

Without going into each CIP Standard – they collectively represent a challenge – both in the identification of assets where the standards will apply, and in the implementation of compliance measures. In these early years of implementation, although the goal is reliability (CIP focused on reliability through security) of the BES, a casual observer might conclude that the goal appears to be proof of compliance. Companies must guard against such intents and conclusions – especially within the personnel ranks of their own companies. If it is not clear from the top of the company – including the Board – that the goal (related to CIP Standards) is reliability/security of the BES, individual employee actions may wander from the real security aspects of the goal. Furthermore, decisions to support proof of compliance may start to trump decisions aligned with accomplishing security. For example, changes to assets so that they no longer are subject to CIP Standards (e.g. installing a “work around” or disconnecting an asset from an IP (Internet Protocol) network for the sole purpose of CIP avoidance) should be examined and reexamined with great care. Non-reporting of assets that should be subject to CIP Standards is also an area of great concern.

At the Board level – at least a discussion of NERC Standards and the company’s compliance plan is appropriate. Within that discussion, special attention to CIP Standards may be warranted given their unique nature. Some questions to ask are:

1. Do we have a CIP Standards Compliance Plan that we can count on now and in the future as standards evolve?
2. Is the 'Tone at the Top' supportive of compliance - and more importantly, is it focused to actually accomplish the levels of security needed?
3. Are the people doing the work equipped with an adequate budget?
4. Cyber security and the CIP Standards are relatively new - do we have the right people to succeed? - are we outsourcing important functions and increasing risk?
5. What role should the Board play with respect to NERC Standards Compliance, and CIP Compliance?

Question 1:

“Do we have a CIP Standards Compliance Plan that we can count on now and in the future as standards evolve?”

This question may trigger a request for Board review of the plan and discussion of the roles of the Chief Compliance Officer and/or the Chief Risk Officer. There should be a discussion of expected future requirements so planning can start now. The Board must satisfy itself that today’s decisions are appropriate for the long term and not just patches to meet the next NERC audit and avoid today’s penalties. The least expensive path to actual security and compliance is most likely a plan which makes the appropriate investments up front rather than relying on a cadence of patchwork solutions.

Question 2:

“Is the 'Tone at the Top' supportive of compliance - and more importantly, is it focused to actually accomplish the levels of security needed?”

This question is important in virtually all business activities – but is critically important in CIP Standards. Management (and the Board as appropriate) needs to ensure employees understand that the key goal is security of the BES and not proof of compliance (although the proof is needed too). This entails both physical and cyber security. Physical security can be costly, but cyber security can be tricky. For example, is Virus Protection software – which still leaves an application open to “Zero Day” attacks (new viruses not incorporated into Anti-Virus protection yet) - good enough? It may seem like a question “down in the weeds”, but the issue points out the need for clear direction on how protected a company wants to be.

Question 3:

“Are the people doing the work equipped with an adequate budget?”

This question seems obvious, but the ensuing discussion can sometimes be revealing – especially with respect to Question 2. For Investor Owned Utilities (IOUs) the challenge is severe. Revenues are sharply down due to the economic downturn – but expenses are largely unrelated to customer usage (except for fuel costs which are largely a pass-through to customers). Also, many companies are pursuing demand response to assemble “virtual power plants” rather than new generation construction because of a long list of difficulties associated with new traditional generation. Regulators too are increasingly pushing for demand response programs as a less expensive alternative to new generation and a customer enabler. Finally, energy efficiency (using less and deriving the same benefits) is increasingly targeted as a way to both help customers control costs and cut CO2 emissions. Energy Efficiency targets are even being legislated – specifying goals that energy companies will have to satisfy. In this environment, how does Management meet earnings needs? Along with cutting budgets to help with earnings – companies must examine where are the budget cuts being made, and where are the remaining budget dollars going? In a time of severe constraints – these problems can many times represent strategic not tactical decisions. Is a real CIP compliance program appropriately funded – to deliver the intended result – BES Security – both now and into the future? If it is not fully funded – what is the risk? These questions need to be addressed by the Board, and where possible, the risks need to be quantified.

For both Questions 2 and 3 above it is useful consider a simile. Consider an invisible “golden thread” connecting the most senior management with the newest employee. It is a thread where management’s intent pervades the entity’s culture, and all personnel derive clues as to how they should make the many decisions they face every day. The message from the top must be clear, repeated, and sincere. Actions taken by the Board and Senior Management and acted out will be heard.

Question 4:

“Cyber Security and the CIP Standards are relatively new - do we have the right people to succeed? - are we outsourcing important functions and increasing risk?”

This question assumes the other pieces are firmly in place and asks the question of whether the job can be accomplished with the people in place. Current personnel must accomplish the task, outsource the task, or a combination of both. Cyber security professionals prefer less rather than more people interfacing with systems. Each person accessing a system is also a potential source of danger (e.g. an engineer making the Substation rounds updating

servers with a software patch from a memory stick). Engineers also prefer fewer changes to critical systems, rather than change something that is working fine. Outsourcing exposes systems to new people who will be gone at some future date. Putting antivirus protection on thin-memory SCADA (network state data collection systems) systems or EMS (Energy Management Systems) servers adds a level of overhead that may be intolerable to system performance.

Standard Antivirus protection itself is questionable. A really professional attack across multiple assets meant to cripple the grid would not likely use a known worm or virus for which a protection mechanism had been deployed. Antivirus technology provides some protection against “new to the world” viruses, but essentially relies on the Antivirus provider first identifying new threats that have been unleashed into the wild. Subsequently, the provider then deploys updates to all customers to defeat the new threat. “Zero Day” is a term that refers to such viruses and the time after they are unleashed and before they are identified by Antivirus providers. It is a time when computers are open to the intended attack. (A technology called “Application Whitelisting” is a solution to this issue.)

Another related question concerns the company’s Information Technology people (who do have experience in cyber protection schemes) – are they involved with the power engineers? Many traditional engineers are excellent at power engineering, but may lack the specialized knowledge to address cyber security – a different subject altogether. On the other hand – Information Technology professionals need to tread with great care on systems that must run 365x24 and sometimes with tight memory constraints. Cross organizational cooperation will be needed.

Question 5:

“What role should the Board play with respect to NERC Standards Compliance, and CIP Compliance?”

Finally, there is the question of the role of the Board itself and what the Board expects of management in terms of information. Related subjects include management goals, compensation, performance metrics, organizational structure related to Internal Auditing, the Chief Compliance Officer, the Chief Risk Officer, and perhaps external auditing groups that are performing pre-Audit services prior to direct NERC Audits. Committee Charters may need to be updated so that the discussion and subsequent Board decisions are captured to inform future Board members. The discussion and decision process can be greatly clarified by using a Responsibility Assignment Matrix (see http://en.wikipedia.org/wiki/Responsibility_assignment_matrix) – making it clear who is responsible for what, both within the Board structures and between the Board and Management.

Conclusion

Protecting the BES against a pervasive attack meant to result in large power outages, and the resultant intended damage to society is, and will be no easy task. CIP Standards are likely to grow both in terms of assets that fall under the CIP rules, and the number of actual standards. Non-compliance can trigger fines as much as \$1M per day per occurrence – and worse – a vulnerable BES. Boards and Senior Management are ultimately responsible and owe their customers the benefits of having a safe and secure BES – which touches on virtually every aspect of everyday life.

The questions and ensuing discussions outlined above are just the start – for a Board that elects an ongoing interface with Management to fulfill their responsibility – there are many more questions to ask as information is provided – and these questions are the subject of another paper.

About the authors

Information Note: the views expressed in this paper are the authors' own and not necessarily associated with any organization that the authors serve in Board, Client, or Advisory Board roles.

Paul Feldman is an independent participant in the energy industry. He is a Director and Chairman of the Midwest ISO, an Independent Director of the Western Electricity Reliability Council (WECC, part of NERC) where he serves on the Board's Compliance Committee, is a member of the National Association of Corporate Directors, and serves on energy company advisory boards.

Shelley Longmuir is an attorney and independent consultant who advises an international client base on regulatory, legal and legislative strategies affecting the global distribution of goods and services. She is an Independent Board member at the Midwest ISO, and a member of the National Association of Corporate Directors.