The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Keeping Up with a Changing World

In the last five years, our electricity industry has seen significant changes. We're seeing a whole new generation mix driven by the reduction in use of fossil fuels and the increasing use of renewable energy sources. Our operational systems are evolving. Non-substation based monitors located mid-span on transmission lines are being used to determine line ratings dynamically. Advanced Distribution Management Systems (ADMS) are driving new efficiencies and increased reliability at the sub-transmission and distribution levels. Synchrophasor measurements are beginning to be used in real-time systems. The technologies that drive our operational systems are being revolutionized by the expanding use of virtualization, containers and cloud computing. At the same time, new threats have arisen, such as ransomware and the public release of advanced cyberattack tools.

However, our current CIP Standards went into effect more than five years ago. Yes, we've seen the addition of Standards for supply chain and for communications security. And we've seen additional, but relatively minor, changes in other areas. But the core fabric of the CIP Standards remains unchanged since mid-2016. The CIP Standards are Reliability Standards, and Reliability Standards change slowly. This is a good thing in many ways. We have a stable set of cyber and physical security Standards that are effective in reducing risk to the Bulk Electric System (BES). On the other hand, some see the CIP Standards as getting in the way of new technologies and new forms of cyber protections. Let's see if there's a way to incorporate some of these new technologies or address new threats while staying within the bounds of compliance with the existing Standards.

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your Entity. It may also help you and your Entity as you strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency and sustainability of your CIP compliance programs. There are times that I also may discuss areas of the Standards that other Entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

Pt Iroquois, MI – Photo: Lew Folkerth

Risk-based Standards

In my opinion, one way to keep pace with the rapid changes our industry is seeing is to develop a risk-based approach to the present CIP Standards. We already have a fully risk-based Standard in CIP-013-1, Supply Chain Risk Management. In CIP-013-1, you're required to develop, implement and maintain a risk management plan for certain areas of supply chain risk. I believe we can adopt risk-based techniques in our approach to compliance for most CIP requirements.

How do we begin? Let's start by choosing one area to improve using a risk-based approach. Figure 1 illustrates some of the areas we might consider. I'll choose a non-prescriptive Requirement, CIP-009-6, Recovery Plans for BES Cyber Systems, R1 Parts 1.3 and 1.4 covering backups and verification of backups.

Next, we'll need to identify the risks that we'll be addressing. This is somewhat backwards to the usual risk approach where we would identify and mitigate the highest risks in our risk register. In this case, one of the classic threats that can be mitigated by performing backups is the loss of a building by fire or other disaster. A new, at least in our context, threat is the encryption of systems and backups by ransomware.

Continued on page 11

Continued from page 10

Plan of Action

Figure 1 shows a modified risk management process. We'll use our known mitigation, backups, to select the risks that can be mitigated by backups. Then we will assess and prioritize these risks and design our backup systems to mitigate the highest priority risks.

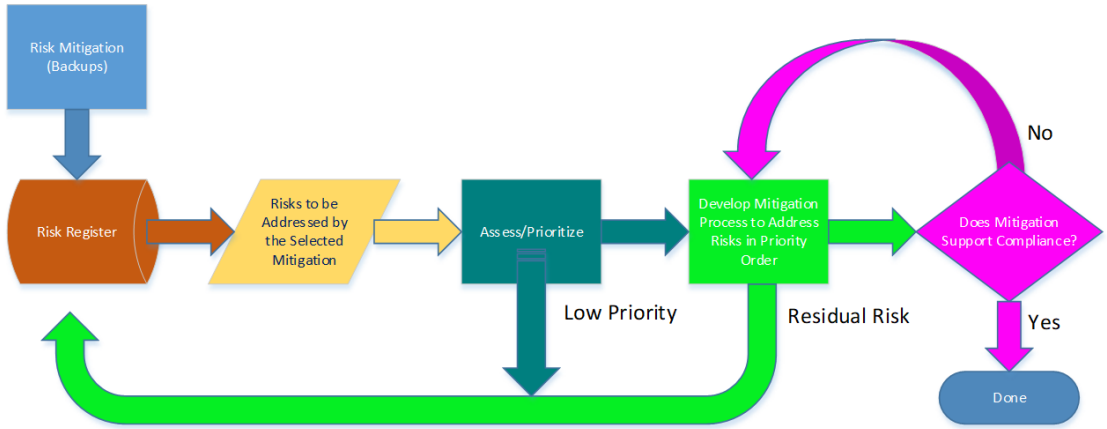

Figure 1

We'll partially mitigate the threat of fire by keeping the backups in a data center that is at a different location than the operational systems we're backing up. Mitigating the threat of ransomware will require a different approach. Ransomware works by encrypting all files accessible to a compromised system. If we keep our backups online, as is common practice, those backups are at risk of being encrypted along with the live files on our operational systems. In addition to keeping our backups at a different site, those backups must also either be offline or not writable by online systems.

When we have a process to mitigate the selected risks, we need to make sure that the process will meet the needs of our compliance program. If not, we need to re-design the mitigation process until it does meet our compliance needs. For example, we will need to make sure that all backup media is stored in a manner that conforms to our information protection program as required by CIP-011-2/3.

Requests for Assistance

If you are an Entity registered within the RF Region and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the RF website here. Back issues of The Lighthouse, expanded articles and supporting documents are available in the RF CIP Knowledge Center.

Candidates for Risk-based Approach

Explicitly risk-based Requirements

- Supply chain
- Communications between Control Centers

Implicitly risk-based Requirements

- Vulnerability assessments
- Malicious code prevention
- Low impact BES Cyber Systems

Less-prescriptive Requirements

- Firewall rules
- Security event monitoring and alerting
- Incident response
- Recovery capability (backups)
- Information Protection

Risks not addressed by CIP (out of scope)

- Below the radar
  - ADMS
- Not operational technology
  - IT/corporate systems
- Historically out of scope but changing
  - PMU/PDC
- Beyond reach
  - Cloud infrastructure

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

Lew Folkerth, Principal Reliability Consultant, can be reached here.