Executive briefing: The role of the executive in CIP compliance

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, resilience 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.

Background on the NERC CIP Standards

The Critical Infrastructure Protection (CIP) standards are part of the NERC Reliability Standards that are mandatory and enforceable for organizations that have an impact on the reliability of the Bulk Power System in North America. The CIP standards set a performance baseline for cyber and physical security for your operational systems. Your organization must meet, and is encouraged to exceed, this baseline.

Operational systems are those systems that control physical assets such as substations and generating plants. They are also the systems that will balance generation with load and ensure the Bulk Power System is operated reliably.

Security is not an end state, it is a set of processes that must be performed to reduce the security risk to an acceptable level. Similarly, compliance is a set of processes that ensure the security processes are performed in a consistent, effective, and timely manner.

Cheboygan Crib Lights, Cheboygan, MI – Photo: Lew Folkerth

Your role as an executive is to select a model to use for addressing cyber and physical security risk and the organizational structure you will use to address that risk. You will also select and support a CIP senior manager who will have the task of implementing and managing the selected structure.

Select a risk model and organizational structure

To start, I suggest organizing your thinking about security risk into three general categories:

- **Business risk** is the risk to the organization, which should include risks to finance, reputation, and staff retention.
- **Compliance risk** is the risk of being found in violation of the NERC Reliability Standards.
- **Security risk** is the risk of compromise or damage to cyber or physical assets.

One of the key differences between the NERC Reliability Standards and other types of standards is the mandatory and enforceable

Continued on page 17

Continued from page 16

nature of the NERC Reliability Standards with financial penalties for violations. The possible financial penalties serve to directly transfer compliance risk to business risk. This is shown in the organizational figures that follow, where compliance risk always impacts business risk.

In my tenure as a CIP auditor and an outreach team member, embedded at times in companies that needed major improvements to their security posture, some highly effective organizations have distinguished themselves. Let's look at some simple models for these organizations and see how they treat risk.

Figure 1 shows the Security group and the Compliance group managed separately. This is also known as a "siloed" approach, where the Security and Compliance groups are in their own silos. The intent of this form of organization may be to have each silo working cooperatively with the other, but in practice this frequently results in a disconnect between the Security and Compliance groups, with less than optimal results from each group.

Figure 2 would seem to be the natural order of an organization, where the Security group is foremost and the Compliance group takes a back seat. However, this form of organization can result in compliance being a bolt-on afterthought to security.

The organizations in both Figure 1 and Figure 2 can result in the Compliance group having insufficient information to demonstrate compliance to the CIP Standards. Also note that in both of the above figures, the Compliance group has no operational duties and is therefore primarily overhead. The next figure explores an organization where compliance adds value to the operation.

Figure 3 shows a type of organization I recommend, where compliance is used as a governance layer for security. In this organization, the Compliance group uses internal controls for governance of security functions. This organization does not make security less important, rather it takes the evidence collection and audit responsibilities off the security staff and places them on the compliance staff. This frees up the security staff to better manage security.

Select your CIP senior manager

The selection of a CIP Senior Manager is an important action. Here are a few thoughts to consider when you make this selection.

The CIP senior manager is a role defined by the CIP standards (see sidebar).

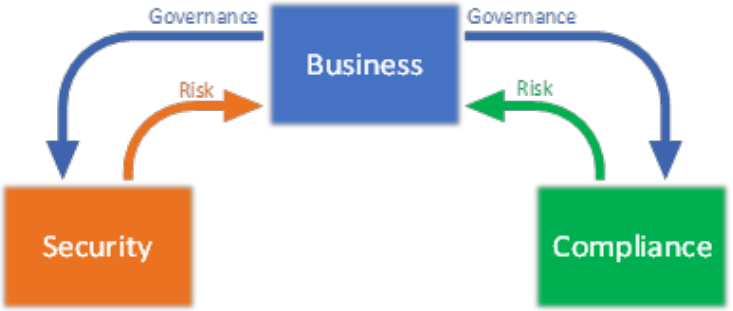

Figure 1 - Separation of Security and Compliance

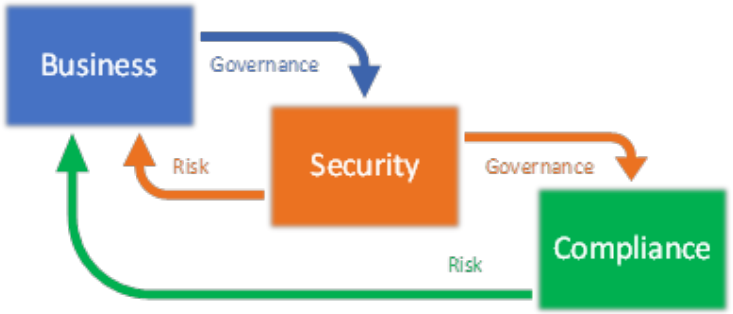

Figure 2 - Security as Governance for Compliance

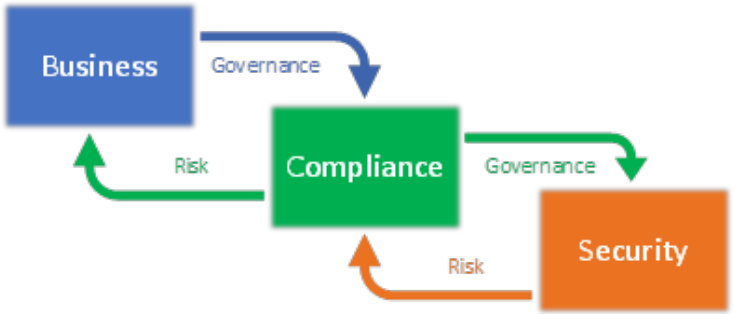

Figure 3 - Compliance as Governance for Security

Continued on page 18

Continued from page 17

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

From *"Glossary of Terms Used in NERC Reliability Standards"*

Simply stated, the CIP senior manager is the person you task with ensuring the CIP standards are applied to your operational systems. You can think of the CIP senior manager as the equivalent of a chief information security officer, but for operational assets rather than information assets.

The CIP senior manager is your eyes and ears into the CIP program and should be your liaison to the Security and Compliance groups. This means the CIP senior manager should understand both security issues and compliance issues and be able to communicate those issues to executives in understandable terms.

Note that the CIP senior manager definition requires that your selection be given both "authority and responsibility" for the CIP program. Too many times I've seen the CIP senior manager given the responsibility, but too little authority to take action. This is like telling your CIP senior manager, "You're responsible for driving the CIP bus, but you don't get a steering wheel."

Support your CIP senior manager

Once you have selected a CIP senior manager, it is important to establish regular communications, possibly via weekly or biweekly briefings. Expect regular updates on compliance and security status, changes to the standards and regulatory environment, emerging threats, staff training and accomplishments, and other topics as needed.

In addition to open channels of communication, you need to provide the CIP senior manager with an adequate budget, staffing, and other business needs.

These actions help set the "tone at the top" that is so necessary to implement effective compliance and security programs in your organization.

You may want to consider treating your compliance program in a manner similar to your safety program, where compliance is given constant consideration, such as "tailgate briefings" before any compliance-related work is performed. I'm in no way saying that your safety program should take a back seat to anything, but only that similar techniques may also produce positive results in the compliance program.

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 Resource Center.

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.