The Lighthouse

Public

By: Lew Folkerth, Principal Reliability Consultant

A Structure for CIP Risk Management Plans

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

As I discussed in the November/December 2018 issue, CIP-013-1 will become effective and enforceable on July 1, 2020. On that date CIP-013-1 will become the first explicitly risk-based CIP Standard. I do not believe it will be the last such Standard. The Project 2016-02 Standard Drafting Team has posted a set of "CIP Virtualization Updates" that are mostly risk-based as well.

Whether a Standard says "[D]evelop one or more documented supply chain cyber security risk management plan(s)" (CIP-013-1) or "[I]mplement one or more documented processes to mitigate the risk posed by unauthorized communications to and from applicable systems…" (CIP-005-7 Draft 1), you will need to have a risk management plan or process in order to fulfill the requirements of the Standard. In this column I'll explore what I think the structure of such a plan might look like.

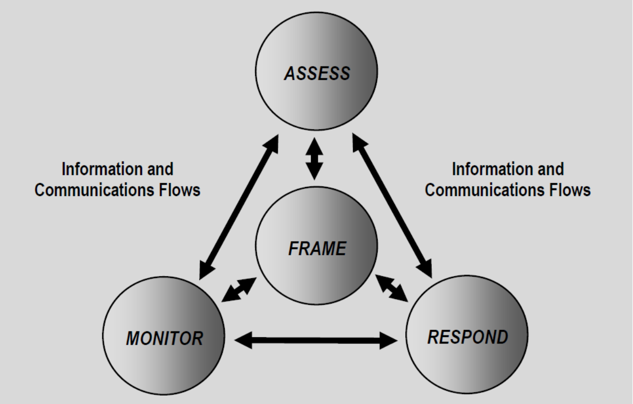

ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

Figure 1: Risk Assessment within the Risk Management Process
Source: SP800-30

Munising Range Lights, Munising, MI - Photo by Lew Folkerth

The structure that follows (see Figure 1) is based on NIST SP800-30, the Guide for Conducting Risk Assessments (found here). I also recommend reading NIST SP800-39, Managing Information Security Risk (found here).

FRAME

Your risk management plan for a CIP Standard should provide a frame for your approach to risk management. The frame provides the context for your risk-based decisions. The frame should contain the following elements:

Scope:

You should carefully identify the scope for your plan. If the scope is too narrow, you risk violating the Standard by not considering all of the required risk areas. If your scope is too broad, you will expend resources and funds that may provide little benefit. You may want your scope to include an inventory of Cyber Assets that are covered by your plan, as well as a list of vendors that may be affected by implementation of the plan (such as for CIP-013-1).

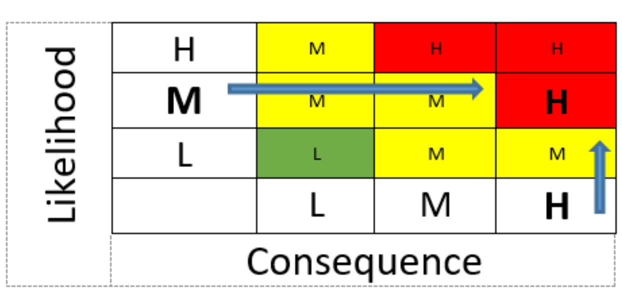
Continued on page 11

The Lighthouse

Public

Continued from page 10

Simplified Risk Assessment Methodology



Likelihood			
H	M	H	H
M	M	M	H
L	L	M	M
	L	M	H
	Consequence		

In this methodology, you qualitatively estimate the likelihood of a risk being manifested and the possible consequence if it does occur. For example, you might assess the likelihood of purchasing counterfeit equipment as medium, and the consequence of implementing such equipment as high. In the methodology above, this would assess as a high risk.

Objectives:

The objectives of the risk management plan should be clearly identified. For example, your CIP-013-1 risk management plan should include the four objectives from FERC Order 850 P2, as well as any additional objectives that are appropriate for supply chain risk management at your organization.

Risk Assessment Methodologies:

The methods you use to assess risk should be spelled out in this section. Each methodology (you can use more than one) will lay out the steps you will need to take to assess the risks you identify. These steps should take into account the inputs to the process (e.g., threat sources, threat events, vulnerabilities, predisposing conditions, etc.). Simpler may be better here (see sidebar), but you will need to select the methodologies that you determine are best suited to your organization. If you create a complex methodology to assess your risks, then you will need to be able to explain that methodology to an audit team.

Definitions:

Any terms used in risk management that may be ambiguous and that are not defined in the Standard should be defined here. Try to keep to generally accepted definitions – unusual definitions will probably be questioned.

ASSESS

Your risk management plan should include a process for assessing risks within the scope of the plan. Volumes have been written about this topic, so I will sketch out a possible outline for a CIP-related assessment.

Identify possible risks:

I think the best approach to identifying possible risks is to cast a wide net and then narrow down the results. Some possible sources of threats include:

- US-CERT
- NCCIC (formerly ICS-CERT)
- E-ISAC
- Vendors

Apply the scope for this process:

Screen for only those risks that are in-scope for this process. For example, one of the risks you identify might be the risk of opening an email attachment and thereby compromising a BES Cyber System.

This technique was used in the 2015 Ukraine attacks and so should be on your list of possible risks. However, this is not a risk that pertains to supply chain cyber security, so it is out of scope for your CIP-013-1 risk assessment. Instead, that risk should be handled by a different risk assessment process.

Apply the appropriate risk assessment methodology:

Once you apply your risk assessment methodology, you should obtain a risk score or risk rating for each identified risk.

Prioritize the resulting risks:

You can't address all risks, so you will need to prioritize the risks you will address. The risk assessment methodology will result in a raw risk score, which you will need to temper with professional judgment. Analyze the risks with the highest ratings and determine how you could reduce each risk. This will help you determine the order in which you address the risks.

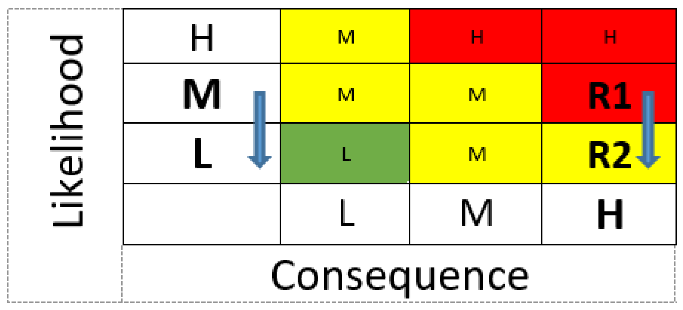
Continued on page 12

The Lighthouse

Public

Continued from page 11

Reducing Risk



Likelihood			
H	M	H	H
M	M	M	R1
L	L	M	R2
	L	M	H
	Consequence		

Based on the previous example, you might choose to reduce the likelihood of purchasing counterfeit equipment by purchasing only from the vendor or from an authorized distributor.

This changes the likelihood of the risk being realized from medium to low and also changes the original high risk (R1) to a medium risk (R2).

Evidence of this risk reduction might include your revised purchasing process that shows the acceptable equipment sources, and purchase orders showing that the process has been implemented.

RESPOND

After you have identified, assessed, and prioritized the identified risks, you will need to decide how to respond to those risks. Those responses should consider the need to produce evidence of compliance. You should also show how the actions you take reduce risk. (See the sidebar, Reducing Risk)

MONITOR

Your risk management plan should include a provision to monitor risk over time. This monitoring should:

- include an ongoing determination of the effectiveness of your risk mitigations,
- identify emerging risks and risks that were not included in the most recent assessment, and,
- ensure that sufficient compliance evidence is being produced and retained.

Disclaimer

If you choose to adopt this framework, you will need to modify it to suit your entity and your circumstances. This framework is intended only to demonstrate one possible approach to address the risk and achieve compliance.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any reliability-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

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

I may be reached here.