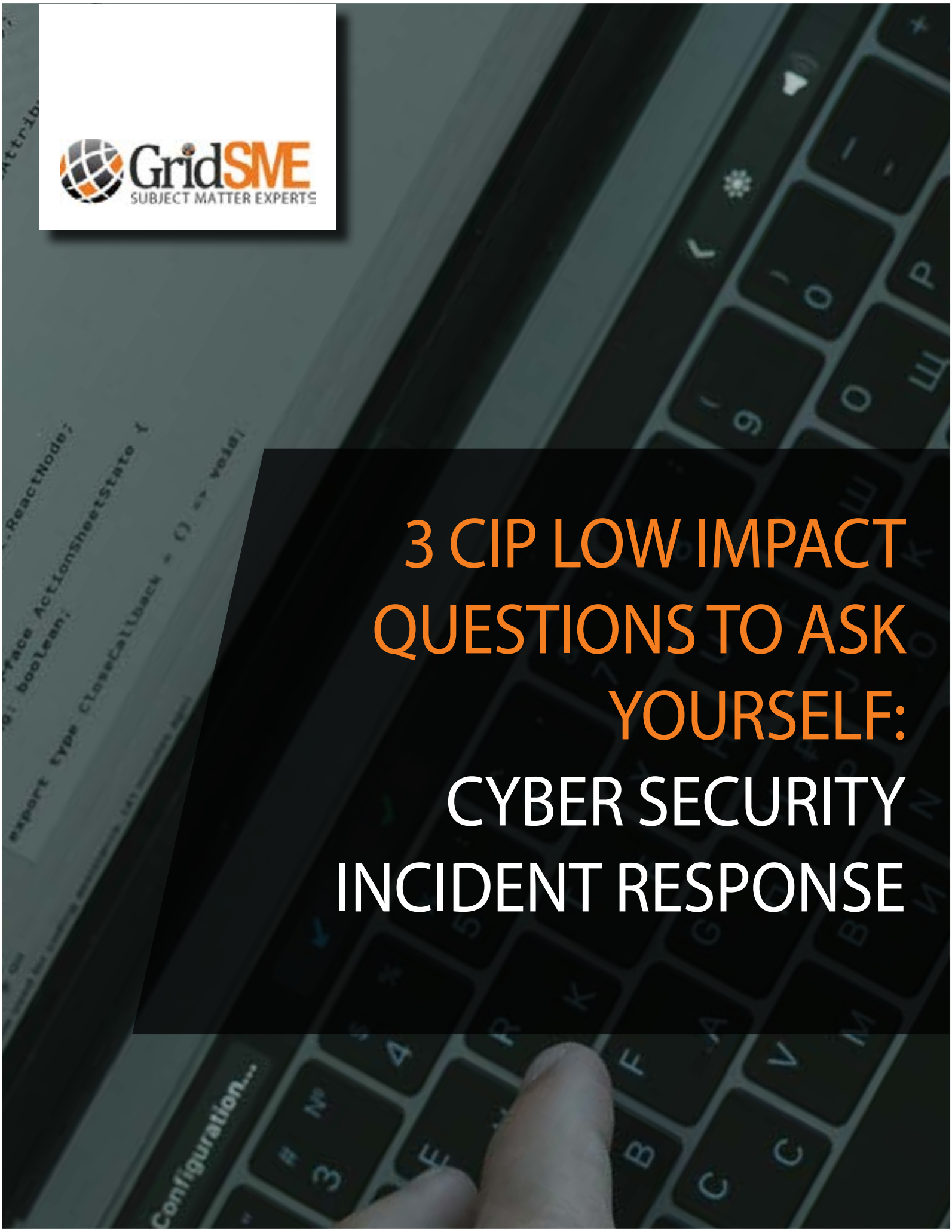


3 CIP LOW IMPACT QUESTIONS TO ASK YOURSELF:

CYBER SECURITY INCIDENT RESPONSE

Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Compared to the rest of the CIP-003-7 requirements applicable for low impact assets, the Cyber Security Incident Response Plan (CSIRP) requirement is arguably the best defined. It also most closely matches the requirements applicable to medium and high impact BES Cyber Systems, so if you already have implemented a CIP-008-6 program, it should be a relatively easy "rinse-and-repeat", at least from a documentation standpoint.

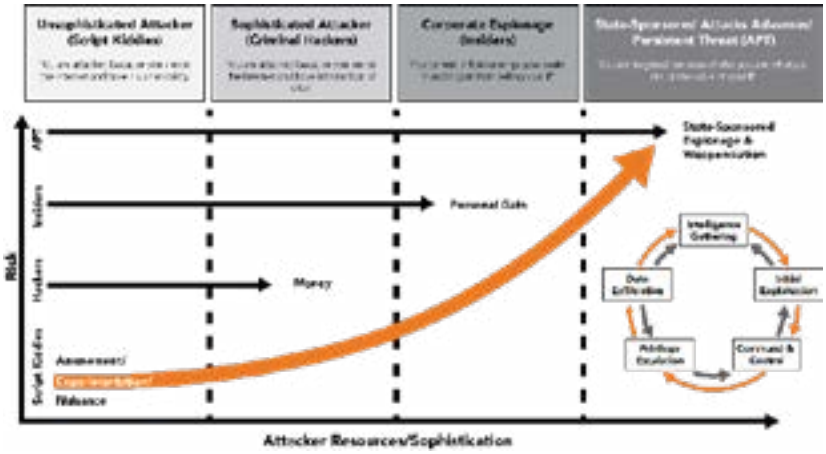
But before we get into the nuances, let's first lets define a Cyber Security Incident, per the NERC Glossary of Terms, as it is applicable to low impact BES Cyber Systems:

> "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System."

How do I identify potential cyber security incidents?

As 4.1 dictates, entities must be able to identify Cyber Security Incidents, which include "suspicious events" that "attempt to disrupt" a low impact BES Cyber System. The terms "identify", "suspicious event", and "attempt to disrupt" are key for the purposes of our discussion.

For better or worse, with the exception of entities which we provide managed security services for, the vast majority of entities I have worked with rely on manual detection methods for low impact BES Cyber Systems--in other words, they rely on operators or engineers to notice "unexplained changes in the availability of a service" or "software crashes and data-base corruptions" and report those as potential Cyber Security Incidents.



If you are completely relying on manual detection methods, you'll most likely never have an identified incident. Unfortunately, that is not because you haven't been breached, but because the objectives of bad actors have change, and so have the associated indicators of compromise (IOC). It used to be that the goal was to breach a system and cause as much disruption as possible. However, especially when talking about critical infrastructure and

nation-state advanced persistent threats (APT), the goal now is to get in and be as quiet as possible to perform reconnaissance and gather intelligence.

As a result, if you think there is going to be a noticeable difference in system performance or behavior that an operator will detect manually, you are unfortunately mistaken.

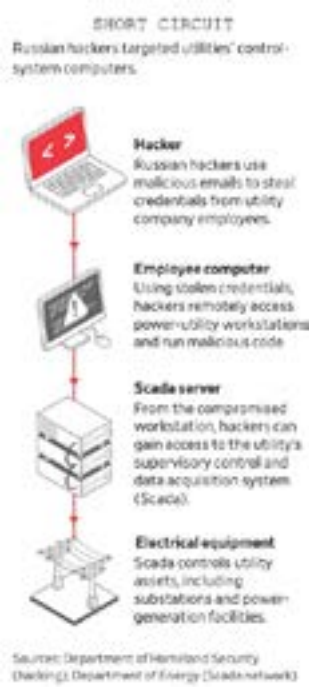
Take the ongoing the events that were made public last year when the DHS and FBI released a report on Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. The report states that this activity has been on-going since at least March 2016, yet the activity was not fully known or disclosed until two years later. There is also evidence that even the utilities that know they were infiltrated have not been able to eradicate the foothold that Russian threat actors have established in their networks to this day.

Similarly, this summer, we are dealing with news that Iran is targeting our critical infrastructure and yet we cannot discern the full scope of impact of this emerging threat.

And before anyone says or thinks that this is just applicable to the "big" utilities, know that according to the Wall Street Journal, targeted phishing (also known as "spear phishing") emails originating from a "15-person company near Salem, Ore., which works with utilities and government agencies, was an early thrust in the worst known hack by a foreign government into the nation's electric grid. It set off so many alarms that U.S. officials took the unusual step in early 2018 of publicly blaming the Russian government."

Take a look at the below map depicting the states in which the targeted companies operate, highlighting the pervasiveness of the campaign.

CALL TO ACTION: if any asset owners or operators are aware, or become aware, of phishing attempts from vendors please do more than just delete the email and/or notify your IT department. Please notify the vendor and encourage them to initiate their incident response plans, as the phishing attempt is potentially an indicator of a serious threat. Depending on the situation, it may be warranted to notify the E-ISAC for information sharing and response purposes.



Back to our regularly scheduled discussion on identifying potential Cyber Security Incidents...

There is one glaring exception in which manual detection methods are very effective: ransomware.

The recent rise in ransomware attacks on small to medium sized municipalities is arguably the most imminent threat to low impact BES Cyber Systems today--if you don't take my word for it, just ask the South African City Power utility who was hit with ransomware a couple of weeks ago. We expect this trend to continue since municipalities are the perfect

targets, as they have valuable data and serve critical functions, yet have limited cyber security budgets and capabilities--and the attackers have been "successful" since the muni's are actually paying the ransoms.

Both types of threats are summarized nicely in Ars Technica's article on the recent rise in ransomware:

"There are two forms of targeted attacks in the destructive world—'I need to be low and slow until I gather the information I need and plan out my attack,' or 'I'm going to drop in, release it, and let it go wild,'" as Christopher Scott, IBM X-Force IRIS' Global Remediation Lead, put it. But the latter are not in the majority. IRIS observed attackers "reside" within targeted organizations' networks for up to over four months before launching their destructive payloads—giving the malicious actors plenty of time to perform reconnaissance of the network and stealthily spread their access. And the attackers will go to great lengths to preserve access to key bits of infrastructure within the network throughout their intrusion, allowing them "to maintain control of their strongholds for as long as possible, and to cause as much damage as they can."

So with all of that said, if you are relying on 100% manual detection methods for your CIP-003-7 Cyber Security Incident Response Plan, you should strongly consider changing your strategy. Manual detection methods are rarely effective at identifying Cyber Security Incidents and, if they are effective, it means it's too late and you have already been breached.

Next week when we cover CIP-003-7 Electronic Access Controls, we will be discussing in detail effective preventative and detective controls that will not only greatly increase your critical infrastructure's cyber security posture, but also greatly improve your ability to detect potential Cyber Security Incidents. In the meantime, here are some very high-level controls to think about to improve your incident response capabilities:

- Centralized logging and alerting (i.e. SIEM)
- Intrusion detection system (IDS)
- Managed anti-virus
- Threat intelligence program

When do I need to test my Cyber Security Incident Response Plan?

If you already have existing low impact assets, hopefully you have already conducted your initial CSIRP test on or before 4/1/2017 when CIP-003-6 went into effect, per the CIP-003-7 implementation plan.

If you have new low impact assets coming online, be sure to conduct your initial test of the plan prior to NERC registration.

Regardless of when you conducted your initial CSRIP test, be sure to retest within 36 calendar months, at the very minimum. Also, as denoted in the

WECC diagram above, and supported by the SANS 6 Key Phases of Incident Response below, be sure to incorporate any lessons learned back into your plan within 180 days of your test.

How should I test my Cyber Security Incident Response Plan?

Entities must, at least once every 36 calendar months, test their CIP low impact CSIRP by one or more of the following methods:

- Responding to an actual Reportable Cyber Security Incident;
- Using a drill or tabletop exercise of a Reportable Cyber Security Incident; or
- Using an operational exercise of a Reportable Cyber Security Incident.

While I have certainly conducted and participated in tabletop exercises that were effective in communicating roles, responsibilities, and the overall high-level incident response process flow, tabletops have notable limitations. For example, while its relatively easy to say "after detecting a malicious file, I will contact the incident commander, begin containment actions, and recover the system from a known-good back-up" its a lot different to actually perform all those actions in a high-stress situation when your critical systems are unavailable.

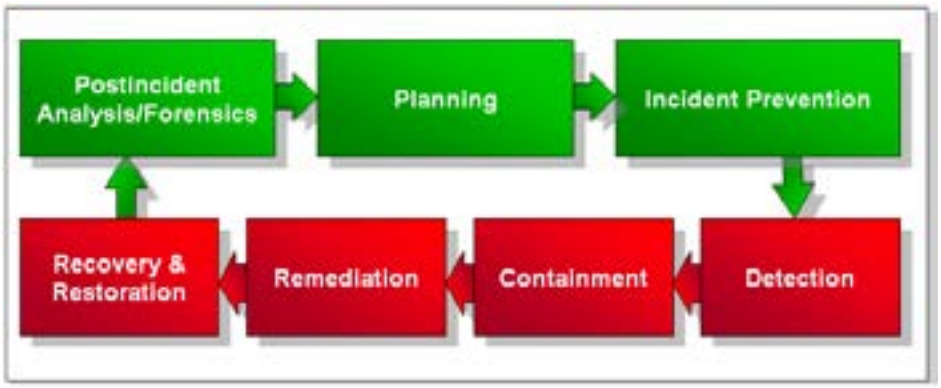
This is why operational exercises are so important. Don't take advantage of the requirement and only conduct tabletop exercises.

With that said, tabletop exercises have a time and a place, and if you are looking for guidance on how to design your own, check out EPRI's Guidelines for Leveraging National Electric Sector Cybersecurity Organization Resource (NESCOR) Failure Scenarios in Cyber Security Tabletop Exercises.

A great way to conduct an operational exercise is to participate in GridEx, a nation-wide exercise designed to execute the electricity industry's crisis response plans through simulated and coordinated cyber and physical security threats and incidents. If you're interested in learning more about the upcoming GridEx exercise, check out NERC's GridEx information page--even if you're organization is not ready to be an active participant, I encourage you to sign up as an observing organization. With minimal effort and commitment required, you can still get a whole host of incident response and preparedness benefits.

My recommendation is to conduct a tabletop as your first CSIRP exercise, then participate in GridEx, then after gaining enough knowledge and familiarity with incident response, take the time and effort to design and conduct your own operational exercise. Reviewing past GridEx reports is a good starting place to understand how to design your own operational exercise.

Regardless of the method(s) you use to test your CSIRP, make sure the test includes responding to a Reportable Cyber Security Incident, and be sure to fully stress test both your proactive (i.e. "left of boom") incident planning steps and the reactive (i.e. "right of boom") incident response steps, depicted in green and red, respectively, in the diagram below from the US-CERT Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability.



Speaking of Reportable Cyber Security Incidents, for those of you with medium and high impact BES Cyber Systems, know that FERC approved CIP-008-6 which expands the reporting requirements to "include incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems." This is in response to FERC's "concern that the existing standards may understate the true scope of threats by excluding from reporting incidents that could facilitate subsequent efforts to harm the reliable operation of the grid."

GridSME
SUBJECT MATTER EXPERTS

DO YOU NEED HELP SECURING YOUR FACILITIES & PROTECTING YOUR INVESTMENT?

SCHEDULE A CALL

OUR SERVICES

- MANAGED SECURITY SERVICES
- MANAGED SCADA SERVICES
- MANAGED NETWORK OPERATIONS
- DESIGN, CONFIGURATION, & ASSESSMENT