Continuous Improvement

By Sam Ciccone, Principal Reliability Consultant

How to use IRPAT to improve your Incident Response Program

The Journey to Security, Resiliency and Reliability

"Ask for help not because you're weak, but because you want to remain strong" – Les Brown

Tabletop exercises and incident response drills are being implemented throughout industry as a way to prepare and train operations and analysis personnel and emergency responders for the wide range of conditions they may face. We love seeing this because we believe it is a great way to preserve and enhance the reliability of the Bulk Power System (BPS). Did you know that RF can help you plan and execute these drills? RF offers the Incident Response Assessment Tool (IRPAT) that can help you test incident response and preparedness capabilities. Here we'll dive into the risks you can self-assess and help mitigate with IRPAT, as well as the benefits you could see on your continuous improvement journey.

How it works

The IRPAT tool provides users the opportunity to evaluate and benchmark their incident response and recovery posture, as well as measure effectiveness by performing simulated cyber or physical incident exercises. It can help characterize an entity's ability to gather and analyze threat intelligence and information from the affected systems and test incident response procedures as they relate to the entity's corporate, BPS, IT and OT environments. It has a repository of current threats with simple to advanced scenarios to test and measure historical performance. For a custom experience, entities can also use the customizable interface to craft relevant cyber and physical test scenarios and conduct tabletop exercises. If you already partake in GridEx, IRPAT can help build on that experience, which is only offered once a year.

The exercises are designed to expose participants to an array of realistic hypothetical scenarios. Here are some of the scenarios participants can explore within IRPAT:

- Denial of Service – Users with proper permissions become unable to access their required information due to cyberattacks. This simulation will present a hypothetical attack that could leave grid operators temporarily blind to generation sites by a cyber event that could potentially impact electric power system adequacy or reliability.
- Dragonfly 2.0 – The Dragonfly group appears to be interested in both learning how energy facilities operate and gaining access to operational systems themselves, to the extent that the group now potentially can sabotage or gain control of these systems should it decide to do so.[1]
- DYMALLOY – Uses common malicious behaviors like spear phishing campaigns to directly target individuals' digital communications and watering hole attacks that place malware on industrial-related websites to steal corporate credentials.[2]
- Other scenarios include ELECTRUM, Ransomware, SANDWORM and more.

What is IRPAT?

- Objectives:
  - Drive consistent, high-quality and realistic exercises
  - Continuously evaluate incident preparedness by utilizing an on-demand database of various cyber and physical security scenarios that go beyond GridEx
- Deliverables:
  - Lessons Learned reports
  - Best practices on incident response and preparedness
- Value add:
  - The ability to learn from a vast database of anonymized incidents

[1] Dragonfly: Western energy sector targeted by sophisticated attack group

[2] Dragos

Continued on page 4

Continuous Improvement

Continued from Page 3

IRPAT Benefits for Entities

- Helps demonstrate annual/periodic testing of incident response and preparedness procedures, as required by CIP-008-6, *(Cyber Security — Incident Reporting and Response Planning)*
- Benchmarks incident response posture and capability against other entities and previously conducted IRPAT assessments
- Offers anonymized lessons learned and best practices as a guide
- Grants access to contact resources for incident response handling (DHS, FBI, E-ISAC, local law enforcement)

Making IRPAT a part of your Continuous Improvement Journey

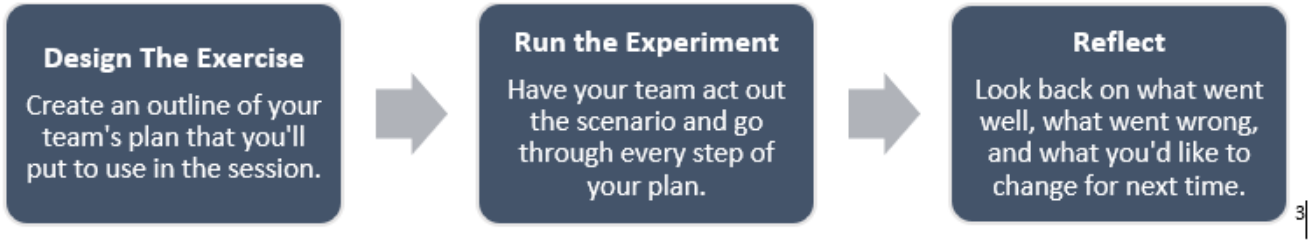
IRPAT and tabletop exercises are effective continuous improvement tools to achieve a resilient and mature incident response plan, and RF can help with training, set-up and facilitation of these assessments. For more information on the IRPAT tool and how to perform this free self-assessment, please contact RF's Entity Engagement department using the form on our website's Contact Us page.

At the end of the IRPAT assessment, the tool generates an extensive report that will provide BPS operators and personnel the ability to identify areas of improvement through deeper insights into components and processes that affect incident response and recovery. These "after action" reports help participants reflect on how the exercise went, documenting incident response areas to improve and initiating those improvement opportunities.

How to maximize IRPAT as a Continuous Improvement tool

Ensure participants are engaged and know their role. This includes the primary participants that are integral to the exercise: a facilitator who keeps the flow of conversation going while trying to get answers and ideas from the participants, an evaluator who identifies improvement opportunities and an observer.

And as you are used to hearing me discuss in this column, the overarching Deming Continuous Improvement Cycle "Plan Do Check Act" (PDCA) also correlates directly to the steps to create and perform a tabletop exercise, as shown below:



[3]

You can also find further information using these additional resources:

Incident Response Preparedness Assessment (RF IRPAT tool information on rfirst.org)

CIP-008-6 — Cyber Security — Incident Reporting and Response Planning

Incident Response Preparedness Assessment Tool (IRPAT)

Incident Response Preparedness Assessment Tool FAQ

GridEx VI - Lessons Learned Report, April 2022

NARUC – Cybersecurity Tabletop Exercise Guide

Crisis Management Tabletop Exercises – A Guide to Success

Do You Use Tabletop Exercises to Improve Performance?

5 Key Benefits from Conducting Tabletop Exercise

[3] How to Create and Run Tabletop Exercises