Continuous Improvement - Incident Management

By Sam Ciccone, Principal Reliability Consultant

The Journey to Security, Resiliency and Reliability

"Houston, we have a problem" – Apollo 13

Lew's Lighthouse article this month discusses Incident Management (IM) and response and the CIP-008[1] NERC standard. This standard's purpose is "To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements." It requires having and implementing an Incident Response Plan.

Incidents on the grid are inevitable. They can be caused by weather, bad actors, human error and equipment error, just to name a few. The key is: How resilient can you be to minimize the damage and get the grid running as normal?

The life cycle of an incident starts prior to event detection (e.g., building resiliency capabilities) and ends in analysis and response. But how do you improve that cycle from start to finish, and how do you improve your IM program? That depends on whether there are incremental changes needed due to incidents that have been known to happen, or are you in crisis mode due to a novel incident that requires significant improvements or even organizational changes? People make improvements happen, leadership empowers people to make the changes, and information and measurement keep the improvement efforts moving.

Continuous Improvement Suggestions and Methods

Your IM program should include the closure of incidents after your organization concludes remediation and the capture of lessons learned from incidents. Lessons learned are particularly important because they can inform your organization on where it can be more proactive to prevent incidents, rather than discovering them after they occur.

Learning from an incident and gleaning valuable information includes involving relevant stakeholders and translating a lesson learned into an action plan for the future. Your organization can utilize these lessons to inform its going-forward strategy, incorporating the lessons into overall grid reliability improvement. And, don't forget scenario brainstorming to consider incidents that haven't been experienced yet, instead of waiting until an incident occurs to learn and prepare.

Capability Maturity Models, Kaizen and Facilitation

Per the "CERT Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience,"[2] the purpose of Incident Management (IM) is: "To establish processes to identify and analyze events, detect incidents, and determine appropriate organizational response."

What are the feeders into IM (see Fig. 1)? CERT RMM discusses the relationships and practices that drive IM. The quality and maturity of these practices plays a direct role in IM and should be evaluated and continuously improved. I encourage you to read more about IM and these process areas in CERT RMM.

The diagram includes External Interdependencies (EXID). EXID play a role in IM, and this is a feeder where many risks to the electrical grid reside. One example risk in EXID is communications. This risk

Figure 1: Feeders into Incident Management

often involves internal, cross-departmental communication, as well as with external entities so that they take action or for general situational awareness. These communications should be anticipated whenever possible and documented in an IM plan. Required communications may span a long list of stakeholders, such as asset owners, IT staff, OEMs, supervisory staff, human resources, regulatory agencies, etc. These external groups may also be able to provide additional perspective not yet considered.

[1] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf

[2] https://www.amazon.com/Resilience-Management-Model-CERT-RMM-paperback/dp/0134545060/ref=sr_1_1?dchild=1&keywords=cert+rmm&qid=1602593262&sr=8-1

Continued on page 5

Continuous Improvement - Incident Management

Continued from page 4

What if you discover after tests, exercises, or actual incidents that your IM process is not effective?

One method of improvement for incidents that have occurred is a Kaizen event to facilitate any needed improvements. Kaizen involves cross-functional brainstorming focused on which of the IM feeders need to be improved. For example, you may find that you need additional resources and technology to improve Monitoring, which will drive more effective mitigation of incidents. For a more effective Kaizen, using an impartial facilitator, or even starting an internal program to develop your own "home grown" facilitators, brings objectivity to the discussion. A good source for planning and executing Kaizen events is "Kaizen Event Fieldbook: Foundation, Framework, and Standard Work for Effective Events,"[3] and a good source for Facilitation is "The IAF Handbook of Group Facilitation: Best Practices from the Leading Organization in Facilitation."[4]

How can we better prepare for incidents we've never seen before?

In the Apollo 13 quote at the beginning of the article, the U.S. space program had never seen such an issue before. Were they lucky they got through it? Or did they prepare for these unknowns? There were seasoned personnel on the ground and in the air, with competencies to react to incidents they never dealt with before. Their high level of competencies allowed them to keep the command module intact, and lives were saved.

For incidents never before seen, building personnel competencies (shown in Fig. 2) is imperative. In the book, "Managing Crises: Responses to Large-Scale Emergencies,"[5] two types of emergencies are discussed: routine and novel. According to the book, crisis (incident) management must be accomplished in novel emergencies. They further detail the competencies necessary for managing novel events and the differences between the competencies and characteristics necessary for routine emergencies. I will delve deeper into Competency Roadmaps in future articles.

So how do the feeders, known events, and never-before-seen events fit into the IM improvement process? Figure 2 depicts this process.

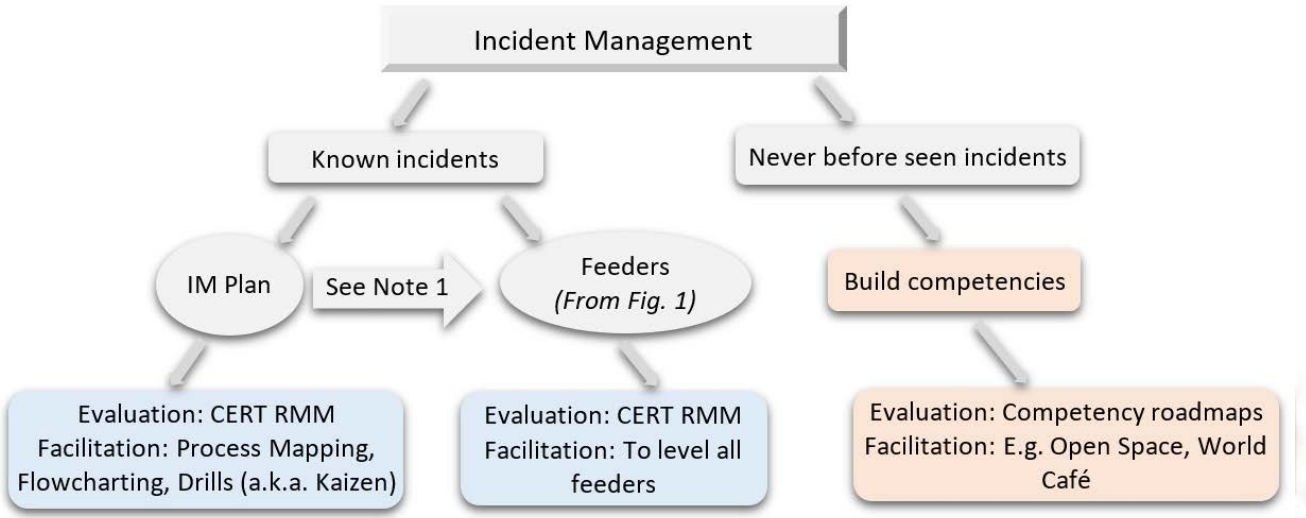
Conclusion

Effective Incident Management is vital to the electric utility industry, especially in today's environment with bad actors trying to hack our cyber systems[6] and those forces physically damaging critical operational assets (weather, foul play.) The methods and information provided here will hopefully give you some tools to improve your IM program.

If you need help facilitating a Kaizen event, creating a Competency Roadmap, or undergoing an Evaluation, please let RF know! You can submit an Assist Visit request to the Entity Engagement team, or you can contact Brian Thiry, Manager, Entity Engagement.

Figure 2: IM Categories and Improvement Activities

Note 1: Target enough feeders that help balance the inputs to the feeders into Incident Management



[3] https://www.amazon.com/Kaizen-Event-Fieldbook-Foundation-Framework/dp/0872638634/ref=sr_1_1?dchild=1&keywords=Kaizen+Event+Fieldbook&qid=1602593068&sr=8-1

[4] https://www.amazon.com/IAF-Handbook-Group-Facilitation-Organization/dp/078797160X/ref=sr_1_2?dchild=1&keywords=the+IAF+Handbook+of+Group+Facilitation&qid=1602593152&sr=8-2

[5] https://www.amazon.com/Managing-Crises-Responses-Large-Scale-Emergencies/dp/087289570X

[6] Related reference: RF's Insider Threat presentation from September 2020: https://rfirst.org/KnowledgeCenter/Workshops/KC%20%20Workshops%20Library/2020%2009-30%20Insider%20Threats%20Webinar%20Presentations.pdf