ICS4ICS
Incident Command System
for Industrial Control Systems

ICS4ICS Exercise at ISA Cyber Security Submit on May 30, 2023

Executive Summary

Mark Boddy facilitated an ICS4ICS Exercise on May 30, 2023, at the ISA OT Cyber Security Submit in Aberdeen Scottland. The exercise participants identified these recommendations:

- Consider issuing Continuing Professional Education (CPE) certificates that would allow exercise participants to maintain their professional certifications
- Develop an IT Disaster Recovery template that asset owners can use to identify options to restore network and other communications that may be impacted by the incident
- Update the exercise materials to explain the difference between a strike force and the other ICS4ICS sub-teams
- Document the need to manage the logistics challenges that the Logistics Section Chief must address to ensure that equipment and staff can be deployed to the appropriate locations; this may include the need for special transportation vehicles, fuel for the vehicles, and safety considerations (e.g., obtain government escort for transportation vehicles)
- Create a template to determine how an ICS4ICS team will ensure staff alternatives are identified including primary, secondary, and tertiary staffing along with external staffing options that may be needed
- Post an example of how medical testing may be needed (e.g., COVID-19)
- Add INJECT to include a criminal investigation which should ensure that the Cyber team limit discussion about cyber issues with ICS4ICS team and do not communicate details in case it is an insider (e.g., the IC and a few people would be aware of the criminal details from the investigation)
- Add more industry specific ICS4ICS Exercises and use past attacks in each industry to create exercise drills and ask the question: Would my company survive this attack?

- Update exercise presentation deck:
    - Slide 77 (Form 204) with multiple sections – need to expand slide to it is easier to read
    - Slide 95 – speaker notes FASC asks “OSC please submit an ICS-213 Resource Request” but next slide has the OSC presenting the ICS-215 Operational Planning Worksheet – Add speaker notes to clarify the 213RR will be create after the current meeting
    - Slide 147 (Print IAP) – need to describe that IAP may be distributed electronically; Ensure that all parties who receive IAP are covered by an NDA (the NDA is normally part of a Mutual Aid Agreement
    - Add a slide at beginning of presentation to review a “glossary” of positions (e.g., IC, SOFR, OSC, etc.)
- Execute Plan & Assess Progress: Ensure to explain that the IAP is being developed for the next operational period; After an incident is declared and we are in the first operational period of an incident, tasks and actions will be taken to manage the incident during that first operational period; The IC/UC will determine if the Incident has been resolved or if another Operational Period is needed); Explain how the Planning P process ends when the incident ends at the direction of the IC/UC
- Ensure Escalation and CIRT procedures explain how the SOC is involved in these processes; Also, explain how the SIEM is used by the CIRT
- Create a resource that explains how BCP is used by the ICS4ICS process
- Continue efforts to engage smaller companies including existing effort with small water, wastewater, and other utilities to help them understand how ICS4ICS can help them manage incident and that it is FREE

Exercise Hot-Wash

Exercise Strengths identified in Hot-Wash

- Explaining what each block in the Planning P was and the work that was to be done followed by the individuals in each position explaining their tasks was more helpful than just going through the PowerPoint.
- Knowing a Delegation of Authority was in place prior to the incident makes the role of the Incident Commander as a decision maker more plausible.
- The ICS4ICS Demonstration underscores the need to have good pre-planning in place prior to an incident.
- Predefined forms results in documentation which provides ~~the~~ context and insights of the “why and how” decisions were made, which can be used later by others (legal, business improvements etc.)

The exercise participants (players) included: Tim Hardwood, Katherine Hutton, Tim Canning, Heidi, Paul Gaynor, Megan Samford, and Heidi Cooke as the scribe.

Detailed Recommendations

These are the detailed recommendations:

- Expecting attendees to take ICS-100 and watching our video(s) prior to a general conference or event is unrealistic. We should plan on Demonstrating the process at these events going forward. If holding an exercise at a company than it is necessary for the participants to have that minimum level of knowledge via ICS-100 and the videos for the exercise to work.
- Changes to existing plan:
    - Setup room with the 3 tables as identified in the PowerPoint. Presentation to be projected close to the Formal Presentation area.
    - Ground Rules, ICS-215, ICS-215A, and ICS-207 taped to wall near Formal Presentation Area leaving room for the agenda, a map (if appropriate), or any other forms the Team deems necessary.
    - Add additional scripting(prompts?) for each position in the ICS4ICS Team to present more in-depth work/conversation and to give the attendees the feeling work is taking place in the background while the facilitator reviews the slides.

- Understanding it is difficult to get 9 ICS4ICS people in the room means we should expect to do this at larger events where ICS4ICS volunteers will have a high probability of attending.