ICS4ICS
Incident Command System
for Industrial Control Systems

ICS4ICS Exercise with Chemical Company on May 2, 2023

Executive Summary

Brian Peterson and Mark Boddy, ICS4ICS program manager and volunteer, facilitated an ICS4ICS Exercise on May 2, 2023, with an anonymous chemical company. The company has an exceptional Emergency Operations Center (EOC) and NIMS/ICS capabilities. The exercise participants identified these recommendations:

- Improve the interface from the Cyber (IT) and OT teams to the EOC
- Include the Cyber and OT team members in future joint exercises with the EOC
- Leverage the mature EOC capabilities, processes, and staff to support future cybersecurity exercises and responses to actual Cyber and/or OT incidents
- Document processes used by the Cyber and OT team to improve their response to actual incidents (see the next page)

Detailed Cyber and OT Recommendations

These are the detailed recommendations:

- Cyber and OT staff work with EOC staff to understand the data they need for their processes, and document those processes. During the exercise, the EOC staff said that they were looking for data from IT/OT/Cyber staff to help them make decisions about safety processes including lock-down; the EOC can repeat their comments about the data they need to make their decisions

- Ensure Safety Officer and other safety staff processes are documented, exercised, and shared widely with everyone involved in incident response and incident management; And are aligned with EOC Safety processes; The ICS4ICS Team had a safety officer who would be working with the EOC safety officer; the ICS4ICS safety officer needs to understand how they will work with the EOC safety officer; exercises will help ensure alignment with the EOC

- There could be a need for multiple Safety Officers with specific knowledge/capabilities as part of the response Team. Document each unique skill of the Safety Team, like staff safety, facility safety, and environment safety. Ensure people have been named to fill each safety role based on their skills and experience. This would make the "Primary" Safety Officer position more administrative in that she/he will take input from the subordinate Safety Officers and keep the EOC Safety Officer updated. These roles should be documented and included in exercises as it is clear the "One Size Fits All" Safety Officer model does not work.

- Share EOC communications processes with cyber and OT staff, particularly as it relates to information sharing with the Crisis Management Team and other company sites. The EOC has processes to manage several communications to the Crisis Management Team, other company sites, the local community, regulators, and other stakeholders: create a document that describes what they demonstrated in the EOC; ensure the document can be used so the IT/OT/Cyber staff don't duplicate any EOC communications AND IF NEEDED provide the EOC with other communications needs and determine who should perform them; Create a brief document that summarizes the communication strategy and who does what (provide input, execute communication, etc.)

- Create a document describing how decisions are made to shut down (or isolate) automation systems at the site and other company sites, and criteria describing when to restart these systems; AND/OR Develop procedures including criteria, and tools to disconnect other automation networks from the enterprise network to protect ICS systems that could be infected by the same malware. Create a Cheat sheet to identify what needs to be checked during an incident; A document that can be review by key management, EOC, and other parties to ensure these decisions are made (criteria, decision authority, etc.) and if needed procedures on how to shut down systems identified as extremely high risk due the existing incident
  See the attached template: ICS4ICS_Shutdown and Isolate Systems Procedure.docx

- Document how staff from other sites may be used to support incident response and ICS4ICS at this site. Then exercise these other staffing capabilities as part of normal exercises.

- Develop a ransomware procedure that describes how Corp Security would work with Corp Legal and how the ICS team would provide them data by investigating the ransomware to determine:
    - How bad is it: Identify the malware and determine if it can be removed from systems
    - How bad can it get: Replication and other ways to spread or impact IT/OT systems and networks
    - Estimate outage period based on recovery time (number of hours or days)
    - Alternatives, if Forensics does not work

  See the attached template: ICS4ICS_Ransomware_Procedure.docx

- Create a list of questions that onsite staff can answer to help remote technical staff understand the problems they are experiencing which will result in faster resolution of these problems.
  See the attached template: ICS4ICS_Onsite Staff Problem Assessment _Procedure.docx

- Evaluate IT and OT Disaster Recovery plans including data recovery

- Consider reducing the Recovery Time Objective for less critical IT and OT systems, so the company can focus on recovering the most critical systems that may affect safety, environment, and/or financial results of the company

- Ensure that critical roles in the IT, OT, and Cybersecurity organizations can be staffed or there is sufficient documentation that would allow junior staff to perform critical functions (e.g., network support, network isolation)