ICS4ICS
Incident Command System
for Industrial Control Systems

ISA

ICS4ICS Exercise
ISA 2024 OT Cybersecurity Summit
June 17, 2024

Executive Summary

Brian Peterson, ICS4ICS program manager, facilitated an ICS4ICS Exercise on June 17, 2024, at the ISA 2024 OT Cybersecurity Summit. Heidi Cooke and Katherine Hutton did an excellent job of capturing notes that allowed us to create this report. The exercise included players and observers from a cross-functional group of 46 people from numerous industries and from various roles including asset owners, product suppliers, consultants, academia, and others. The exercise participants identified these recommendations:

- More resources and materials are needed to engage management explain the value of the ICS4ICS Program so they can allocate resources to support the deployment of ICS4ICS and fulfill their role in delegate authority
- Procedure templates and ICS4ICS processes need to be updated to clarify that some decision teams require delegation of authority from Executives (CMT) to determine who is the ultimate decision maker and when CMT approval is required
- Roles and responsibilities of the ICS4ICS Team, CMT, and related teams needs to be document in a RACI
- Provide a single form to capture decisions, activities, and action items during a cyber incident including data normally captured in the NIMS/ICS Forms
- Update Declaration procedure to define attributes of a cyber and non-cyber incidents, and update Incident Commander Job Aid with link to information
- Update Escalation Procedure template to define severity of incidents and roles that will be activated and when to pre-notify the next severity level team members
- Update ICS4ICS Implementation Guide to include cross training of ICS4ICS Team members to ensure people can handle multiple roles

- Update PIO Job Aid to ensure messages (media, employee, community, investor, government reporting, and others) are aligned and consistent; and consider that the message will be seen by the adversaries
- Document that external communications must be timely and accurate, AND must only include factual data with limited conjecture
- Update ICS4ICS Exercise materials based on feedback:
    - Define risks associated with exercise scenario: OT and business operations are shutdown, and not limited to loss of buildings where staff work
    - Update exercise to include summary slides for process templates
    - Update exercise to include more information on Unified Command
    - Add information about potential (e.g., mental) health impacts to ICS4ICS Team, update job aids to reflect the requirement to monitor health of staff
    - Include description of transfer from 1st to 2nd shift
    - Explain (IAP) plan is developed for next shift while also working actions to resolve incident including CIRT/SOC works while ICS4ICS Team is planning
    - Add slide describing how to maintain ICS4ICS capabilities, including frequency of exercises and initial and on-going training
    - Add slide for Gov Reporting with examples for reporting requirements: EPA, FEMA, and other government agencies
- Update Cyber Insurance procedure template with information from exercise notes
- Update Gov Reporting templates to reflect when evidence must be collected (e.g., laws or regulation evidence requirements) and evolving EU reporting requirements
- Update templates for BCP/DR and Ransomware to clarify risk of backup data and recovery processes being corrupted
- Update Job Aids to ensure staff are ready with a go-bag including medicine, etc.
- Document GDPR requirement when collecting phone numbers for escalation
- Create a guide on how to evaluate and manage company policies to address incidents, ICS4ICS, IT, OT, etc.
- Update contracts with critical vendors, services providers, and consultants to have them participate in ICS4ICS exercises
- Update PIO Job Aid to include vendors, investors, and others in the communication plan (requires alignment with teams responsible for those relationships)
- Create a procurement guide with incident management requirements: RFI/RFP, contract, and manage the vendor/3rd party

Detailed Notes and Findings

Management Engagement

- Important to discuss with management ICS4ICS processes and their involvement so there is a process in place that they understand
  - Important to define who is in charge up front so during an incident there is clarity about executive leadership ownership and participation
  - ACTION: We need to develop a MLM for executive staff and potentially a brief job aid
    - Ensure the CMT understands that they appoint an Incident Commander who leads ICS4ICS, but CMT may want to be involved
    - Explain the decision teams defined in procedure templates and the need for the CMT to appoint a decision maker for each
  - ACTION: Clarify in documentation the type of incident: IT vs. OT vs. other
  - ACTION: Understand what Incident Command System plans already exist and who is responsible for each type of incident: IT, OT, Fire, etc.
    - Need right person appointed to be IC for each type of incident
- Keep executives busy so they have work and aren't micro-managing
- Culture changes in the company may be critical to support Cyber Incident Response and ICS4ICS
  - Management must learn to live with the decisions of the Incident Commander including declaring an incident, engaging vendors and other 3rd parties and associated costs to the company, etc.
    - The Crisis Management Team (CMT) who are C-level staff must appoint a senior person to the Incident Commander roles who is someone they trust to make decisions on their behalf
    - The CMT needs to define decisions that require their review and/or approval which can be based on the costs associated with the decision, the potential operational and financial impacts, significant safety related decisions, etc.
    - The CMT will require periodic reporting from the Incident Commander so they can stay abreast of the situation and decisions being made
  - ACTION: MLM for CMT includes risks of declaring and spending money on a non-incident. Also, address business risks of containment

Executive Leadership Engagement messages/focus:

- NIMS/ICS Overview
- Org structure and how 4 sections and officers work together
- Span of Control
- IC decisions must be support (may affect decision about who is selected to the IC)
- May need to call out importance of Finance and Admin

ADDITIONAL COMMENTS AFTER THE EXERCISE:

Management must learn to live with the decisions of the Incident Commander

This is engrained in OPA90. The Qualified Individual (Initial incident commander, they receive the initial notification from the ship / facility), is legally authorized to make decisions, engage 3rd party vendors, activate resources, and commit funds on behalf of the company. There is no asking for permission to start spending money during an incident it is understood that boats will splash without delay. This of course goes along with resources must be in line with what the incident is required, and you obviously don't get hired again if you screw that up. Maritime responses are of course significantly more simplistic; how long is the ship, well then you need this much boom and this many tugs....

Incident Commander Authority and Decision Teams defined in procedure templates

- Incident Commander is the ultimate decision maker and should have procedures that define who and when they need approvals for some high cost or risk decisions
- The Executive Team (Crisis Management Team) may want to make some decisions that may result in significant risk to the company or may have significant financial consequences

Roles & Responsibilities

- RACI chart of responsibilities is needed
  - Recommend creating the RACI so it can be used during the planning phase
  - Obtain sign-off from management
- Responsible vs. Accountable must be clear
  - Responsible = role focused on executing the task
  - Accountable = role that owns the task and is responsible for the outcome
  - ACTION: Create a RACI as an example that can be included in the ICS4ICS staffing and planning materials
- ISA99-WG-15 is looking at the competency of the various roles which should be aligned with the ICS4ICS developed RACI
  - Determine what additional models and external resources are needed to define the competencies – potentially focus on ICS4ICS Work Force Develop (WFD) Assessment tools (20+ roles)

NIMS/ICS Forms

- Forms are guides for what data needs to be collected during an incident
  - ACTION: Create a template to capture data during the incident AND show how it relates to the NIMS/ICS forms >> this is often used for shift turnover
    - ensure form includes data required for team, mgmt, other reporting
    - create an example of the forms after 12-hour 1st shift
    - These forms are not just guides >> data must meet legal requirements
      - EU, Europe, and Canada all have reporting requirements that are coming through new laws and regulations

Escalation-Notification-Declaration Procedure

- Need to determine when there is a cyber or non-cyber incident
    - ACTION: Update Declaration Procedure template to define attributes of an incident
        - ISA99-WG-16 (Bryan Singer) is working to define attributes of an incident
        - Define for: Asset Owner vs. Service Provider vs. Product Provider
    - ACTION: Update Incident Commander Job Aid
- Declaring an Incident requires understanding non-cyber incidents:
    - ACTION: Update Declaration Procedure template to include a flowchart helping the CIRT and Incident Commander determine the type of problem we are having (to these bullets)
        - Operational failures (e.g., pump)
        - Process failure (e.g., HMI logical failure)
        - Hardware problems (e.g., servers, cables, etc.)
- Declaring an incident may result in costs for a non-incident
    - ACTION: Create procedures to define when an incident should be declared
- Bronze, Silver, Gold structure for intercompany notifications (P0 to P4 – high to low)
    - Bronze – normal operational incident that likely can be handled in a limited amount of time with a limited amount of people and other resources
        - Bronze is handled by operational team
        - Escalate to Silver team to keep them informed and let them know they may be activated if the incident cannot be resolved quickly
    - Silver – more complex incident that requires leadership from non-operational managers
        - Silver is managed by management (non-operation level team)
        - Escalate to Gold team to keep them informed and let them know they may be activated if the incident cannot be resolved quickly
    - Gold – extremely complex incident that would likely also require staff from outside parties who provide cyber expertise (e.g., Dragos, Mandiant, etc.)
        - Gold is managed by senior management and requires higher level of communications to various parties
        - Escalate the Crisis Management Team to ensure they are aware and engaged
    - Need to consider what operations team does while communication and notification is happening because you don't want operations to stop and wait before doing work while communications are being developed/pushed
    - ACTION: Update Escalation Procedure template to include Bronze-Silver-Gold (look at other terms Yellow-Orange-Red based on team feedback)

ADDITIONAL COMMENTS AFTER THE EXERCISE:

When does an event move to become a cyber incident?

With regards to Event Vs Incident, this one troubled me when we talked about it a long time ago. It seemed there was great concern over calling something an incident because of the ramifications for notifications, timelines, and insurance etc., however, this is more of a business concern opposed to a technical definition. I think we do need to be technical in our definition because business decisions are often very clouded.

I read the following on an ISC2 forum post, and I think it hits the nail on the head for the technical definition, but if business leaders and management want to nitpick whether something is truly an incident in their case and environment then I don't think our community will be able to come to an agreement. Perhaps we need a 3rd category of "Reportable Incident".

Event - Any occurrence that takes place during a certain period
Incident - An event that has a negative outcome affecting the confidentiality, integrity, or availability of an organization's data.
https://community.isc2.org/t5/Tech-Talk/Event-or-Incident/td-p/38973

Just for an oil example in the USA – if it creates a sheen, it is reportable. However, for oil, there is the International Maritime Organization and the International Convention on Oil Pollution Preparedness, Response and Co-operation (OPRC). Is there a widely accepted international organization that has defined Event Vs Incident? I think our definition needs to be broad because every business will view this differently and it will certainly differ across international/state borders.

Is there a good source that you are aware of that documents the issues, particularly for insurance / notifications, that begin once an event is determined an incident? Though we are international, I don't think it is wrong to focus on the US requirements for starters and then ask the group of international SMEs to provide documentation on requirements elsewhere.

Training and Staff Readiness

- Train ICS4ICS members on more than one role (particularly above their position) so they can step up quickly to perform the role (this is common practice in the military)
    - ACTION: Update the ICS4ICS Implementation Guide to include cross training (identify the roles that are potential backups: SOFR > OSC > IC)

Communications

- Organizations need to understand that internal communications may be exposed publicly as part of a government investigation so internal messages must be reviewed and approved using the same processes and scrutiny as public messages
    - ACTION: PIO Job Aid – messages must be aligned and consistent
- Communications plans should include strategies on how and what to communicate to adversaries (e.g., the party requesting ransom)
    - ACTION: PIO Job Aid – messages must be developed with the awareness that the adversaries will also see the message
- All Messages about the incident (which are always developed by the PIO) must be based on the facts with no speculation
    - The content of these message may be used by the government and others which could result in fine, penalties, lawsuits, and other negative consequences for the organization
    - PIO guide should include information about how to write communications describing a potential incident AND reinforce the concept of stick to the facts only
- No team member except the PIO can share communications with the media or communicate to them in any form (this is described in our procedures/exercises)
    - UNLESS the PIO arranges media-meetings and prepares specific staff members to participate in those meetings
- Legal environment is moving toward putting pressure on organizations to ensure they have timely and accurate public messaging – this is designed to ensure processes will last through the test of time
    - ACTION: Update PIO Job Aid – external communications must be timely and accurate but should be limited to factual data with limited conjecture

ADDITIONAL COMMENTS AFTER THE EXERCISE:

Members can reach out other companies to see if they have an interest in getting involved with the ICS4ICS and our exercises. We always referred our clients to certain consultants for maritime responses. Major companies already have relations with a media consultant for crisis management.

ICS4ICS Exercise Materials

- Important to make OT System impact assessment clear up front in the exercise to demonstrate the level of impact that triggers ICS4ICS
  - ACTION: Exercise needs a slide describing impact: OT and business operations are shutdown; not about loss of buildings where staff work
- The screen was too small to see the process templates (MS Word) >> there is a need for PPT slides with large bullets to summarize each process template
- Exercise Room setup was challenging because the monitor was very small and difficult to read for the 50+ attendees
  - We should summarize the process templates in PPT slides that are easier to read
  - Consider simulating virtual rooms (e.g., MS Teams rooms) during the exercise
  - Add comment that many organizations use virtual meetings to accomplish the ICS4ICS and Cyber Incident Response activities
  - ACTION: update PPT to include summary slides for process templates
- Add definition of UC
  - ACTION: update PPT to include more information on UC
- We must take care of our people – mental health (occupational health)
- Staff participating in the ICS4ICS Team and/or the Cyber Incident Response Team are at great risk of having health issues related to stress from 12-hour shift and the demanding work they must perform
  - The ICS4ICS leaders and officers must monitor their staff for possible stress related problems and prevent them when possible
  - Primary – Secondary – and – Tertiary staff must be trained to perform each role; other people on the team should learn the role(s) of others including more senior roles
  - ACTION: update PPT to include health risks to people staffing ICS4ICS Team
  - ACTION: Ensure job aids reflect the requirement to monitor the health of staff (already included in WFD job tasks)
- Change "INT" to "Intelligence" (page 67 or so)
  - UPDATE: PPT
- ACTION: Add comment: Risk Assessment was completed as part of incident planning
  - This will limit conversations about other risks outside of the ICS4ICS exercise scenario
- When transferring responsibilities to 2nd ICS4ICS shift (slide 159) Communications needs to remind next shift that all media interactions MUST be handled by the PIO
  - ACTION: Update PPT describing transfer to 2nd shift
- Planning Cycle Planning-P is worked while also working in parallel preparing for next 12-hour shift
  - Preparing for 2nd shift AND
  - Working on the actual incident
  - ACTION: Add slide to PPT

- Need to explain that CIRT/SOC continue to work to solve the problem and investigate, remediate, and recovery; AND handle whatever they find or new data points
    - ACTION: Add 1-slide to PPT describing CIRT/SOC continue working
- Frequency of exercises is likely 6-months (staff turnover, memory, etc.)
    - ACTION: Add slide describing how to maintain ICS4ICS capabilities

Insurance

- Address these questions on Cyber Insurance:
    - What to expect from the insurance company including likely possible reimbursement for costs (labor, ransom, equipment, vendor support, etc.)
    - Need to define terms like and concepts for:
        - Initiation payment to insurance company when declaring an incident
        - Requirement for Finance to understand the insurance policy
        - What costs (OT, IT, labor, vendors, ransom, etc.) are typically covered by an insurance policy?
        - Provide examples of when not to contact your insurance company, like if Ransomware is not covered
        - ACTION: Add topics/questions to Cyber Insurance procedures
- Asset Owners should determine the type of cyber insurance their suppliers (products, consultants, integrators, etc.) have that potentially can help the Asset Owner to respond to incidents and/or cover incident costs
    - Determine how cyber insurance of supplier may impact asset owner

Government Reporting

- Add requirements from EPA, FEMA, and other government agencies to PPT slides
    - ACTION: Update PPT for Gov Reporting to include gov agencies
- Need to understand when evidence must be collected (e.g., laws or regulations required the collection of data which is likely tied to government reporting requirements)
    - ACTION: Update ICS4ICS guide to address this topic
- EU cyber incident reporting defined in NIS2 requires reporting incident to the government within 72 hours
    - Germany is defining their specific NIS2 requirements as an EU member state
    - UPDATE: Gov reporting to include NIS2

Ransomware

- Ransomware “justification process” should include
    - Ransomware often destroys backup data
    - Backups and recovery procedures should be retained on a platinum disk (Write Once Read Many) and must be tested periodically (typically every 6 to 12 months) to ensure data can be restored from the backup media using the restore procedures
    - Agent of Chaos (HBO movie) describe cyber incident research and type cyber incidents
        - https://www.politico.com/newsletters/weekly-cybersecurity/2020/09/21/inside-the-hbo-doc-agents-of-chaos-790512
    - ACTION: Update templates for BCP/DR and Ransomware to clarify risk of backup data and recovery processes being corrupted

Staff Readiness

- Ensure staff are ready with a go-bag including medicine, etc.
- Staff should have a jump-bag (go-bag) with key resources (medicine, water, etc.) that they can take with them to make a 12-hour shift for ICS4ICS Team
    - ACTION: Update Job Aids to describe need for go-bag

Data Privacy Concern

- GDPR compliance when collecting personal phone numbers?
    - ACTION: Determine GDPR requirement when collecting phone numbers

Policies

- Review IT policies and OT policies to ensure they are aligned and provide guidance that can be used during an incident
- IT policies are not always fit for purposes in the OT environment, so policies to manage processes for both environments should be assessed and updated
    - ACTION: Create a guide on how to evaluate and manage company policies to address incidents, ICS4ICS, IT, OT, etc.

ADDITIONAL COMMENTS AFTER THE EXERCISE:

I will say that from the perspective of a penetration tester OT environments are in no way secured to the same extent that IT environments are and there is a big problem with getting some folks to understand that the old arguments of isolation, serial communications, etc., don’t really fly any more when you start hooking up ‘smart’ devices. As much as companies hate it, they really do need to start securing their OT environments, maybe even patch them 😀.

Supply Chain

- Vendor contracts (e.g., SCADA/DCS Maintenance) need to include requirements for the vendor to support incident management including participating in exercises
- Vendors are critical and need to participate in exercises: Ensure you also verify the chain of command (e.g., not have vendors report to each other)
  - Ensure vendor staff are changed > consider named vendor staff
  - Contract with vendor must include requirements to have them participate in exercises
  - ACTION: Update contracts with critical vendors, services providers, and consultants to have them participate in ICS4ICS exercises
- Need to include 3rd party (vendors, investors, etc.) in IRP communications plan
  - ACTION: update the PIO Job Aid to include vendors, investors, and others in the communication plan (which likely requires alignment with various teams)

ADDITIONAL COMMENTS AFTER THE EXERCISE:

Need to include 3rd party (vendors, investors, etc.) in IRP communications plan

I didn't catch if we already do this, but for the sake of exercises, making a point to announce/communicate that "Good thing we pre-populated a lot of this stuff with our known vendors, local hospital/fire/EMS".

- We must understand the IRP of supply chain because they might become part of the response effort; this also means understanding when critical responsibilities and insurance lie with third parties
    - Law in Canada will likely require asset owners must have visibility into their supply chain and the associated risks >> will SBOMs be required?
    - ACTION: Create a procurement guide with incident management requirements: RFI/RFP to contract thru to managing the vendor/3rd party

ADDITIONAL COMMENTS AFTER THE EXERCISE:

US DOE introduces supply chain cybersecurity principles to bolster global energy infrastructure security ... https://industrialcyber.co/supply-chain-security/us-doe-introduces-supply-chain-cybersecurity-principles-to-bolster-global-energy-infrastructure-security/#:~:text=The%20DOE%20Supply%20Chain%20Cybersecurity%20Principles%20also%20prescribed%20that%20end,continued%20availability%20of%20supplier%20technical – This will directly speak to one of the topics covered today.

While talking about firms better managing supply chain third-party risk, we need to make sure were not trying to do too much. TPRM is hard. Make sure you have a good program in place (to manage TPRM). Also, it is worth noting that conventional wisdom is that you cannot control your third-parties security (hard enough to control your own 😊). They have vendor relationships in place (that you don't control). You can ensure they have a good program in place, though! I agree with making this program comprehensive, but we need to make sure we are not trying to conquer everything

Information Requested by Participants

These are the links we agreed to provide based on discussions at the exercise:

ISAGCA.org WFD curriculum paper (Heidi) CURRICULAR GUIDANCE: Industrial Cybersecurity Knowledge link to learning resources https://www.isasecure.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/Industrial%20Cybersecurity%20Knowledge%20FINAL.pdf?hsLang=en
ISA99 WG-15 Work Force Development working group (Heidi) To join ISA99 Standards effort for specifically on Workforce Development (WFD) with ISA/IEC62443 : ISA99WG15 Please contact EBrazda@isa.org to request to be added to WG15 meetings. To participate in ISA standards there is no cost.
ISO 27000 whitepaper (Heidi) Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA_Applying%20ISO-IEC%2027001-2%20and%20the%2062443%20Series_White%20Paper.pdf
UK has JESIP (Tim Canning) JESIP Link: https://www.jesip.org.uk/
ICS4ICS WFD documents and opportunities to provide feedback (Brian) See attached file that summarizes job roles that are critical to ICS4ICS along with their key tasks. Also attached is a spreadsheet that provides more details that align with the summary. I also included PowerPoint project presentation.
Andre slides on ISAGCA and Site Assessment See attached file
EU Regulations that are currently being evaluated by ISAGCA (Brian) See next table

European Union Cybersecurity Initiatives
EU Cyber Resilience Act
NIS2 Directive
IACS Components Cybersecurity Certification Scheme
Radio Equipment Directive (RED) EN-18031-1/2/3 (standard)
Machinery: Regulation (EU) 2023/1230
Cybersecurity Act - European Union (restricted URL) Includes: Regulation 2019/881 - EUR-Lex
2021/0106(COD) - 21/04/2021 - Artificial Intelligence Act
Directive (EU) 2022/2557 of the European Parliament