Protect: Incident Response (IR) Plans

`

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

2.S: Does the WWS have a written cybersecurity incident response (IR) plan for critical threat scenarios (e.g., disabled or manipulated process control systems, the loss or theft of operational or financial data, exposure of sensitive information), which is regularly practiced and updated?

Recommendation: Develop, practice, and update an IR plan for cybersecurity incidents that could impact WWS operations. Participate in discussion-based (e.g., TTX) and operations-based (e.g., Drill) exercises to improve responses to potential cyber incidents.

Why is this control important?

The cybersecurity IR plan is essential in helping your WWS recover quickly from cybersecurity incidents. The IR plan describes the strategies, resources, and procedures to prepare for and respond to a cyber incident. You can incorporate the IR plan into the Emergency Response Plan (ERP) and use it as part of contingency planning (see Factsheet 5.A).

Implementation Tips

Identify personnel, OT and IT support staff, and vendors that your WWS should include in the development or update of the IR plan.

Develop the cybersecurity IR plan to include the following:

- Defined roles and responsibilities and actions that all WWS personnel will take during and after an incident.
- Procedures to operate the WWS in manual mode, or alternate procedures to maintain water service if an attack compromises the OT system.
- References to other relevant response plans and procedures as needed.

Additional Guidance

✓ A good starting place to develop an IR plan is EPA’s “Incident Action Checklist for Cybersecurity”. Conducting regular drills and exercises, such as tabletop exercises, is essential for an effective emergency response to minimize adverse impacts from a cyber incident. WWS should plan and conduct exercises with the participation of WWS staff, OT and IT support staff, vendors, and emergency response partners. If drills and exercises are new to the WWS, use a scenario that is simple and realistic. For example, develop a scenario that is based on a ransomware attack, since it is a common attack method. The goal is to exercise and evaluate existing plans, policies, and procedures and update them with any lessons learned. Conducting exercises will also help build the WWS’s cyberattack response capabilities. After conducting the exercises, the WWS should hold an exercise debrief. The debrief provides an opportunity for exercise participants to provide feedback on what happened during the exercise and any obstacles/challenges encountered, and to identify any gaps in the WWS’s plans, policies, and procedures that it needs to address.

- Diagrams and other visuals to help all WWS personnel understand their roles, responsibilities, and actions.
- Template forms that WWS personnel can use to record decisions, actions, and expenditures.
- Procedures and contact information for where to report the incident (see Factsheet 4.A)

Distribute the IR plan and train all WWS personnel on the new cybersecurity procedures or steps in the IR plan by conducting drills and exercises.

Review the IR plan annually, at a minimum, and make changes as needed, such as changes in staff, vendors, and contact information.

Update the IR plan after any significant changes to OT and IT systems and based on any lessons learned from an exercise or actual incident.

Resources

EPA's Incident Action Checklist for Cybersecurity: Provides a rip-and-run style checklist to help WWSs prepare for, respond to, and recover from cyber incidents. *https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf*

WaterISAC's 15 Cybersecurity Fundamentals: Page 35 provides information and resources to develop an IR plan. *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

NIST Policy Management Template Guide: See Incident Response Policy. Incident Response Policy template that utilities can leverage to develop and Incident Response Policy. *https://www.cisecurity.org/wp-content/uploads/2020/06/Incident-Response-Policy.docx*

CISA's Cyber Incident Response tools: Provides incident response training and playbooks. *https://www.cisa.gov/cyber-incident-response*

EPA's Tabletop Exercise Tool: Provides users with resources to plan, conduct, and evaluate tabletop exercises. *https://ttx.epa.gov/*

CISA Tabletop Exercise Packages (CTEPs): Provides tools for stakeholders to conduct planning exercises on a wide range of threat scenarios. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios. Provides users with resources to plan, conduct, and evaluate tabletop exercises. *https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages*

CISA's Top Cyber Actions for Securing Water Systems: See item 5 on page 2 of this resource for additional information. *https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems*