Protect: System Back Ups

`

COST: **$$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

2.R: Does the WWS backup systems necessary for operations (e.g., network configurations, PLC logic, engineering drawings, personnel records) on a regular schedule, store backups separately from the source systems, and test backups on a regular basis?

Recommendation: Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections. Implement the NIST 3-2-1 rule:

3) Keep three copies: one primary and two backups;

2) Keep the backups on two different media types; and

1) Store on copy offsite.

Why is this control important?

Backups are a critical element of your WWS's restoration and recovery activities in the event of a cyber incident, hardware malfunction (e.g., hard drive failure), or physical destruction of equipment (e.g., fire, flood). Backups are one of the most important first lines of defense to avoid having to pay ransoms and quickly restore operations.

Implementation Tips

Identifying all operational, customer, employee, financial, and other data that your utility may lose or that an attacker may corrupt during an incident is crucial for restoring normal operations post-incident. Regularly backing up OT/IT systems ensures you can recover to a known and safe state in the event of a compromise. Implementing the NIST 3-2-1 rule is essential: keep three copies of your data (one primary and two backups), store backups on two different media types, and keep one copy offsite to safeguard against local incidents like fire or flood.

Protect backup media by storing it separately from the systems being backed up whenever possible, using off-site, cloud-based backups, or manual backup rotations, such as swapping out multiple backup drives periodically with one always stored off-site.

Additional Guidance

- ✓ The WWS should perform backups using the "backup-in-depth" approach, with layers of backups (e.g., local, facility, disaster) that are time-sequenced such that recent local backups are available for immediate use and secure backups are available to recover from a large cybersecurity incident. The "backup-in-depth" approach relies upon a utility having three copies of their data, utilizing at least two different storage media, and storing at least one copy remotely offsite or in the cloud. The WWS should use multiple backup/restore approaches and storage methods to ensure that backups are rigorously produced, securely stored, and appropriately accessible for restoration.

`

Establish a procedure to ensure the backup process is followed on a specified schedule and file backups are usable. Regularly test backups to confirm they are effective, spot-checking the file size and modification date of backup files on recovery media, and validating the ability to recover files individually.

For OT assets, ensure backups include elements such as PLC logic and HMI graphics to enable quick restoration of these critical components.

At a minimum, backup and test OT and IT systems annually to ensure the reliability and effectiveness of your backup and recovery procedures.

Resources

NIST Standard 800-82 Rev. 3, Guide to Operational Technology (OT) Security: Additional information on backups can be found in Section 6.2.4.3 (page 112). *https://csrc.nist.gov/pubs/sp/800/82/r3/final*

NIST Standard 800-34, Contingency Planning Guide for Federal Information Systems: Additional information on general backup procedures and best practices can be found in Section 3.4.2 (page 21). *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf*

CISA’s Top Cyber Actions for Securing Water Systems: See item 6 on page 2 of this resource for additional information. *https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems*