REDUCING THE CYBERSECURITY RISKS OF PORTABLE STORAGE MEDIA IN OT ENVIRONMENTS

Portable storage media continue to be useful tools for transferring data physically to and from Operational Technology (OT) environments. Universal Serial Bus (USB) flash drives are commonly used, in addition to external hard drives, CD or DVD drives, and other removable media.

Though portable storage media are convenient, their usage poses cybersecurity risks for operational environments. Procedural, physical, and technical controls are important for minimizing the likelihood of a cyberattack from portable storage media usage. The National Cybersecurity Center of Excellence (NCCoE) has developed cybersecurity considerations to help OT personnel use portable storage media securely and effectively.

PROCEDURAL CONTROLS

An organization should develop policies that enforce:

- Purchasing, authorizing, and managing organization-owned media. Devices provided by other sources should be considered untrusted.
- Procuring devices that support hardware-based encryption standards such as FIPS.
- Prohibiting media usage unless expressly authorized. Authorization should be limited to specific personnel and purposes.
- Procedures for provisioning, usage, storage, sanitation, and destruction.
- Enable logging for traceability (e.g., system and user identity, device serial number, date and time).
- Training staff on policy and procedures.

PHYSICAL CONTROLS

One way to minimize risk when using portable storage media is to apply physical controls for accessing, labeling, and storing them.

- Media should be stored in a physically secure location where only authorized individuals can access.
- Approved portable storage media should be labeled. Labels may indicate:
  - Who may use it
  - On which network/system it may be used
  - Functional purpose

Having a designated space to store approved media, in conjunction with access control and labeling, is a foundation for a well-implemented set of physical controls.

NIST Special Publication
SP 1334 ipd (Initial Public Draft)
https://doi.org/10.6028/NIST.SP.1334.ipd
July 2025

TECHNICAL CONTROLS

Media should be protected consistently with guidance found in NIST SP 800-82. An organization should establish technical controls that enforce:

- Blocking or disabling ports (e.g., USB ports, CD/DVD drives) on unauthorized machines. This could be done using physical blocks or logically disabling devices and ports.
- Scanning of media prior to and after usage.
    - Automatically scan media with updated malware detection software.
    - When inserting media into devices that don't support scanning, consider alternatives such as kiosk scanning solutions.
- Reformat devices before reusing them on different equipment or environments.
- Write-protection when files only need to be read.
- Disabling Autorun.
- Encrypt the data stored on portable storage media using FIPS-compliant algorithm.

TRANSPORT AND SANITIZATION

Transportation within and between organizations introduces risk, which can be reduced by applying additional physical and logical controls, including:

- Encryption or a locked container can be used to securely transport USB devices within an organization.
- Hash or checksum verification should be performed when transporting files (e.g., between the integrator and the asset owner).
- Sanitation should be performed prior to disposing of the device. Media sanitation should include monitoring, reviewing, approving, tracking, and documenting actions. For more details, see NIST SP 800-88, Guidelines for Media Sanitation.

CONCLUSION

Organizations can reduce the cybersecurity risks of USB device use with secure physical and logical controls on the access, storage, and usage of USB devices, and training on how to utilize USB devices safely and effectively in OT environments.

For more information on specific controls, please refer to Guide to Operational Technology (OT) Security (NIST SP 800-82), Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53), and Guidelines for Media Sanitation (NIST SP 800-88).

LEARN MORE

For more information about NCCoE Manufacturing, visit: https://www.nccoe.nist.gov/manufacturing

@NISTcyber

linkedin/showcase/nccoe