Salas O'Brien

OT Cybersecurity Checklist

This checklist serves as a roadmap for reviewing multi-layered cybersecurity measures in operational technology environments.

CONTRIBUTOR
Julie Liu, Governance & Risk Specialist
OnShore Security

Layer 1: Oversight and Governance

- [ ] OT Security Team to provide governance and oversight throughout the lifecycle of system design, including architecture, procurement, installation, configuration + maintenance, and decommissioning.
- [ ] Maintain a list of legacy OT systems whose hardware and software components are no longer supported by the vendors and have a plan to sunset these systems.
- [ ] Follow a process and tools to track, monitor, and maintain audit logs of all maintenance activities of OT assets. Activities tracked include access and authentication.
- [ ] Use OT Incident Response plan. Our plan addresses data breach notification and reporting requirements.
- [ ] Create a risk management process that addresses the impact OT systems may have on personnel safety and the environment, as well as interconnected OT systems and the supply chain.
- [ ] Vet our suppliers and service providers and measure their capabilities, trustworthiness, internal security practices, their supply chain relationships, and their dependencies.
- [ ] Incorporate secure architecture design principles for our OT systems including the ability to separate the OT network from the corporate network, failsafe capabilities, and ensuring resiliency.

Layer 2: Physical

- [ ] Incorporate physical security control to protect physical locations.
- [ ] Incorporate physical access controls to keep all computing and networking equipment in secured areas.
- [ ] Keep OT systems in production in the "Run" position unless being actively programmed.
- [ ] Monitor physical access to OT systems through electronic surveillance systems that store and record either the physical presence or the lack of physical presence of individuals.
- [ ] Track the location of people and OT assets to ensure that they stay in authorized areas and can easily identify personnel who may need assistance especially in the case of an emergency.

Layer 3: Network

- [ ] Isolate OT assets from our IT assets. We segment our OT network using security levels and/or security zones.
- [ ] Centrally log OT asset activities and have monitoring, alerting, and incident reporting capabilities.
- [ ] Regularly monitor and review these logged activities with a centralized Security Incident and Event Management (SIEM) system.
- [ ] Regularly scan our OT assets to assess status and identify vulnerabilities.
- [ ] Monitor OT network traffic for anomalies.
- [ ] Incorporate principles of Zero Trust Architecture into our OT systems.

Layer 4: Hardware

- [ ] Keep an inventory of hardware associated with our OT systems.
- [ ] Track and maintain the state of OT hardware devices using embedded technologies such as the Trusted Platform Module.

Layer 5: Software

- [ ] Use application “allowlisting” to prevent non-authorized applications and services from executing in the OT host environment.
- [ ] Have an efficient process to deploy patches to OT environments that minimally or better yet does not impact OT system operations.
- [ ] Practice Secure Software Development throughout the entire software development lifecycle.
- [ ] Harden the OT systems according to our documented secure configurations. Any changes to these configurations go through a change control process.
- [ ] Build fail safe features into the software that controls our OT systems.