ASIS INTERNATIONAL
Utilities Security Council

IT SECURITY COUNCIL

ITSC Top 6 Control Systems Security Recommendations

1 Document physical security system configuration

Document physical security system configuration using the same best practices as the rest of the enterprise.

a. Depending on the organization, this may be self asserted or may be a 3rd party highly regulated audit
b. Includes system and device documentation and configuration (network as-built diagrams and firmware revisions)

2 Follow a planned maintenance procedure

Follow a planned maintenance procedure that realistically addresses segmentation and physical security software compatibility issues while addressing the defense of the underlying network infrastructure.

a. Patches, anti-virus
b. Capability for remote monitoring and scanning
c. Continuity of operations and service level agreements (SLAs)

3 Use standards based technology

Use standards based technology particularly with cryptography, and whenever possible maintain a validated interoperable infrastructure.

a. Multiple interoperable implementations (at least three vendors)
b. Standards based cryptography (PKIX, TLS)
c. Multi-factor authentication (for example using Radius, PIV, FIDO)

4 Maintain and measure vendor supply chain

Maintain and measure vendor supply chain to ensure that it is healthy and capable of supporting the deployment on an ongoing basis.

a. Principal point-of-contact (goals and measures, other relationships, buy maintenance)
b. Integrators and service providers (help desk, escalation, training, credentialing)
c. Vendors (interoperable components/services, help desk, escalation, training, credentialing, APIs)

5 Treat data within physical security infrastructure as sensitive enterprise data

Treat data within physical security infrastructure as sensitive enterprise data to protect confidentiality.

a. Jurisdictions, industries, use cases
b. Dependent on data infrastructure, platforms and applications
c. Data security
d. Data privacy

6 Follow the vendor's best practices

Follow the vendor's best practices regarding deployment and use of their solutions.

a. Documentation (for example, sample configurations)
b. Hardening guide (proper configuration and documentation of ports, protocols, etc.)
c. User Forums
d. Roadmap, general availability, and end-of-life