STADIUM SPOTLIGHT: **Connected Devices and Integrated Security Considerations**

Sports venues use connected devices to facilitate business operations, fan experience, and a safe environment for patrons. These devices allow stadium personnel to access and manage various business information systems, industrial control systems (ICS), and communication systems essential to daily operations. While connected devices bring many benefits to stadium operations, a single compromise of a connected device could provide an access point into a stadium's network, potentially compromising critical systems or services. The Cybersecurity and Infrastructure Security Agency (CISA), in partnership with the National Center for Spectator Sports Safety and Security (NCS^4), developed this infographic to provide examples of how potential activities of malicious cyber actors could impact stadium operations. This resource does not intend to encompass all risks to stadiums.

Video Board and Public Address (PA) System

Vulnerability: A stadium's control system is unsecured, leaving its video boards and PA system vulnerable to hackers.

Consequence: Hacker displays or announces threatening message, causing crowds to panic.

Automated Lighting Controls

Vulnerability: A stadium's lighting control system fails to implement remote access authorization only on a need-to-have basis.

Consequence: Nefarious actor shuts down lighting in the stadium, causing patrons to rush out of the stadium and endangering lives.

Point of Sale (POS)

Vulnerability: A stadium vendor network has outdated and unpatched software or firmware.

Consequence: Hacker disables POS systems, resulting in loss of revenue and dissatisfaction among patrons.

Stadium Entrance Equipment

Vulnerability: A control system operator account lacks strong password protection.

Consequence: Malicious actor prevents entrance into the stadium by hacking into the stadium's control system and locking all turnstiles, causing mass gathering that makes the crowd vulnerable to a mass attack such as a bombing or active shooter.

Electric Vehicle (EV) Charging Stations

Vulnerability: A charging station's control and safety system lacks firewall protection.

Consequence: Nefarious actor obtains credit card information of charging station patrons, compromising personal information. Actor displays threatening message on EV charging station, causing patrons to panic.

Small Unmanned Aircraft System (sUAS)

Vulnerability: A stadium's sUAS, which is used to support stadium operations, lacks an encrypted data link and strong encryption keys.

Consequence: Malicious actor introduces malware that distributes a denial-of-service attack, congesting networks and rendering dependent systems inoperable.

Telecommunications

Vulnerability: A stadium's telecommunication system lacks network segregation or other similar protective technology.

Consequence: Cyber attacker disrupts telecommunications, impairing communication with law enforcement and emergency services, resulting in delayed response times.

Closed-Circuit Television (CCTV)

Vulnerability: A stadium's CCTV system does not have properly segregated and isolated access controls.

Consequence: Malicious actor disrupts CCTV and telecommunications, impairing communication with law enforcement and emergency services, resulting in delayed response times.

Heating, Ventilation, and Air Conditioning (HVAC)

Vulnerability: A stadium's HVAC system lacks network segregation or other similar protective technology.

Consequence: Cyber attacker raises the temperature in a server room and servers become overheated, rendering them inoperable.

Fire and Emergency Management

Vulnerability: A stadium's fire and emergency management system is unmonitored.

Consequence: Hacker sets off fire alarm system, causing patrons to panic and rush out of stadium, putting lives at risk.

Smart Grid

Vulnerability: A stadium's smart grid meter memory, containing administrator credentials, lacks encryption.

Consequence: Nefarious actor manipulates meter settings, resulting in the stadium losing power and potentially shutting down critical systems.

Stadium Kiosk

Vulnerability: A stadium kiosk's firmware lacks password protection.

Consequence: Cyber attacker shuts down ticketing system, causing unrest among patrons due to the inability to purchase tickets or be granted admission.

STADIUM SPOTLIGHT:
Connected Devices and Integrated Security Considerations

ENTERPRISE LEVEL RISK MITIGATIONS

Once stadium Chief Security Officers and Chief Information Security Officers analyze risks, security teams should develop measures to minimize vulnerabilities to the enterprise by implementing security policies, training and exercises, and encouraging collaboration. Consider the enterprise risk mitigation strategies below.

- **Conduct a facility assessment to identify** physical security and cybersecurity vulnerabilities and develop a risk-based approach to stadium security. Connect with CISA's Protective Security Advisors and Cybersecurity Advisors for help planning, coordinating, and conducting security and resilience surveys and assessments.
- **Employ fundamental cybersecurity best practices and standards** for enterprise networks and ICS, such as multi-factor authentication. Communicate these policies and procedures to staff to increase enterprise resiliency.
- **Develop and implement an insider threat mitigation program** to reinforce a culture of shared responsibility and asset protection. Refer to CISA's Insider Threat Mitigation Guide for more information on establishing an insider threat prevention and mitigation program.
- **Develop and implement employee training and exercises** to ensure on-the-ground personnel are equipped to identify, report, and respond to suspicious behavior and cyberattacks with physical consequences.
- **Ensure stadium policies prohibit persistent remote access,** monitor all remote connections to the network, and investigate and validate every communication to a new Internet Protocol (IP) address or domain from the control system environment.
- **Formalize collaboration** across organizational security functions and integrate physical security and cybersecurity best practices into standard processes. Refer to CISA's Cybersecurity and Physical Security Convergence guide for a framework for developing a holistic security strategy.
- **Consider an operational technology (OT) cybersecurity manager** to collaborate with vendors, integrators, and contractors during the lifecycle of the OT and information technology (IT) process, and serve as a liaison between cybersecurity and physical security teams.
- **Leverage CISA's tools and resources** to help identify vulnerabilities that malicious actors could exploit.
- **Subscribe to CISA** Cybersecurity Alerts and CISA Insights to stay up to date on threat vectors.

ASSET LEVEL RISK MITIGATIONS

Enterprise risk mitigation strategies should extend to securing connected assets (e.g., stadium kiosks, POS terminals, and EV charging stations). These strategies include updating device software and firmware, monitoring equipment, and securing physical access points to assets. Consider the asset risk mitigation strategies below.

- **Develop logical network segmentations** to create divisions between IT and OT systems and limit cross-access to devices and data, mitigating the consequences of a successful cyberattack.
- **Disable any unnecessary ports and ensure proper network scanning** for rogue or ad hoc wireless access points to protect against credential harvesting, and update and patch software to provide enhanced security.
- **Control and configure Wi-Fi networks** only through network management and the control plane, and disable public wireless networks when not in use.
- **Consider the use of a software bill of materials** to ensure software security and supply chain risk management.
- **Secure physical access points to networks and systems,** including building security systems. Maintain detailed access control logs and asset management lists.
- **Employ a multi-step security approach** by authorizing remote access only on a need-to-have-basis, implementing two-factor authentication, and ensuring the use of a virtual private network (VPN).
- **Monitor equipment** for signs of physical access or tampering (e.g., unknown devices connected to On-Board Diagnostic II ports, spliced wires, or indications of a removed dashboard) and report suspicious activity.
- **Protect each connected device** by changing default settings, creating unique passwords, enabling encryption, and keeping hardware, software, and firmware updated.
- **Consider participating in CISA's Enhanced Cybersecurity Services (ECS) program,** which protects IT networks by offering intrusion detection and prevention services through accredited service providers.

RESOURCES

Mitigation and Guidance:

Catalog of Bad Practices: cisa.gov/BadPractices

ChemLock: cisa.gov/chemlock

CISA Cybersecurity Awareness Program Small Business Resources: cisa.gov/publication/stopthinkconnect-small-business-resources

Commercial Facilities Resources: cisa.gov/cisa/commercial-facilities-resources

Cyber Essentials Starter Kit: cisa.gov/cyber-essentials

Cyber Resource Hub: cisa.gov/cyber-resource-hub

Cybersecurity and Physical Security Convergence: cisa.gov/publication/cybersecurity-and-physical-security-convergence

Cybersecurity Best Practices for Industrial Control Systems: cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems

Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems: cisa.gov/publication/cybersecurity-best-practices-operating-commercial-unmanned-aircraft-systems

Get Your Stuff Off Search (S.O.S.): cisa.gov/publication/stuff-off-search

Insider Threat Mitigation Guide: cisa.gov/insider-threat-mitigation

Known Exploited Vulnerabilities Catalog: cisa.gov/known-exploited-vulnerabilities-catalog

Public Venue Security Screening Guide Touchless Screening Annex: cisa.gov/public-venue-security-screening-guide-touchless-screening-annex

Security and Resiliency Guide and Annexes: cisa.gov/security-and-resiliency-guide-and-annexes

Security Convergence: Achieving Integrated Security: cisa.gov/security-convergence-achieving-integrated-security

Securing Public Gatherings: cisa.gov/securing-public-gatherings

Securing the Internet of Things: cisa.gov/uscert/ncas/tips/ST17-001

Shields Up: cisa.gov/shields-up

Stop Ransomware: cisa.gov/stopransomware

UAS-Critical Infrastructure: cisa.gov/uas-critical-infrastructure

Unauthorized Drone Activity Over Sporting Venues: cisa.gov/publication/unauthorized-drone-activity-over-sporting-venues

Assessments:

Critical Infrastructure Vulnerability Assessments: cisa.gov/critical-infrastructure-vulnerability-assessments

Cybersecurity Advisors: cisa.gov/stakeholder-risk-assessment-and-mitigation

Protective Security Advisors: cisa.gov/protective-security-advisors

Training and Exercises:

Counter-Improvised Explosive Device Training and Awareness: cisa.gov/bombing-prevention-training

Critical Infrastructure Exercises: cisa.gov/critical-infrastructure-exercises

Cybersecurity Training and Exercises: cisa.gov/cybersecurity-training-exercises

NCS⁴ Training & Education – DHS/FEMA Courses: ncs4.usm.edu/training/fema-dhs-courses/

TEEX Training and Education – DHS/FEMA Courses: teex.org/

Incident Reporting:

CISA Incident Reporting System: us-cert.cisa.gov/forms/report

FBI Internet Crime Complaint Center IC3: ic3.gov/

United States Secret Service Field Offices: secretservice.gov/contact/field-offices

For more information or to seek additional help contact us at **Central@cisa.gov**.