ACADIA TECHNOLOGY GROUP

STADIUM CYBERSECURITY BEST PRACTICES ASSESSMENT

STADIUM TECHNOLOGY AND ASSOCIATED RISKS

Recent advances in stadium technology have improved life safety, increased the reliability of industrial controls and enhanced the integrity of sporting events. While these technologies improve the fan experience, they also pose cybersecurity risks that require a rigorous application of best practices. Stadium Operations, which now uses the same systems technology as Corporate Operations, must now evaluate cybersecurity threats and apply appropriate risk controls.

Further, the recent convergence of industrial control systems, such as lighting, key-card access and HVAC, over IP networks presents unique challenges to protecting reliability and life safety. In the past, all of these systems were standalone islands with vastly different technologies. Today, they can be managed centrally with an IP network used as a backbone to transport the traffic. This presents the risk of exposing these systems to attacks from the outside world and the same threats that IP corporate networks deal with today.

Stadium Security Best Practices

The Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) formed a working group with commercial facilities experts to produce stadium security best practice guidelines. **These guidelines address specific risk areas of stadium systems confidentiality, integrity and availability.**

Stadium Cybersecurity Best Practices Assessment

Acadia Technology Group collaborated with a major sports franchise venue to develop an assessment that aligns with NCCIC stadium security best practice guidelines. Acadia now provides an executive-level or deep-dive assessment that reviews the current state of risk and control for key systems and processes with the goal of providing business-case guidance to remediate risk.

QUESTIONS TO CONSIDER

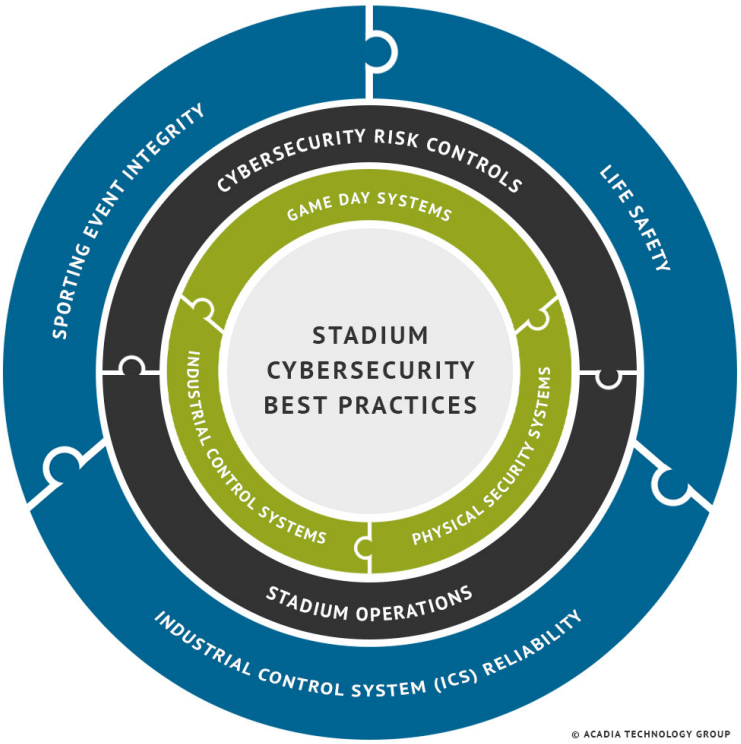
- **Are you following the NCCIC cybersecurity guidelines today?**
- **What are your gaps?**
- **Are you prepared for a review by a Major League Organization?**

The Assessment At a Glance:

- The focus is on industrial control systems, enterprise systems and communications systems.
- Interviews and artifact collection are used to evaluate the level of readiness and risk controls.
- The assessment highlights areas of best practice that are strong and weak.
- It will help you reduce your risks and prepare for the future.
- It identifies high-level gaps and resource allocation suggestions.

Note: *Most stadiums have outside tests done to physical security controls and/or penetration tests to corporate systems; this engagement is tailored specifically to stadium-centric cybersecurity best practices as defined by the NCCIC.*

973-233-1260 www.acadiatech.com info@acadiatech.com



SECURITY IS YOUR RESPONSIBILITY.

The merging of stadium life safety, game day and industrial control systems around Internet IP networks has brought considerable cost savings and efficiencies while also exposing the environment to IP-based threats. Stadium risk managers must continuously adopt cybersecurity best practices that control risks to life safety, game day integrity and stadium industrial controls.

Acadia's Stadium Cybersecurity Best Practices Assessment provides risk managers and CIOs/CISOs with a fixed-cost, short-term engagement that will identify high-level gaps and suggest where resources should be allocated.

START YOUR ASSESSMENT

In the coming year, stadium risk managers will be expected to show due diligence towards managing these threats and risks by adopting cybersecurity controls and best practices as outlined by the NCCIC. The Stadium Cybersecurity Best Practices Assessment is the best place to start – contact us to request your assessment.

CONTACT ACADIA

973-233-1260 www.acadiatech.com info@acadiatech.com