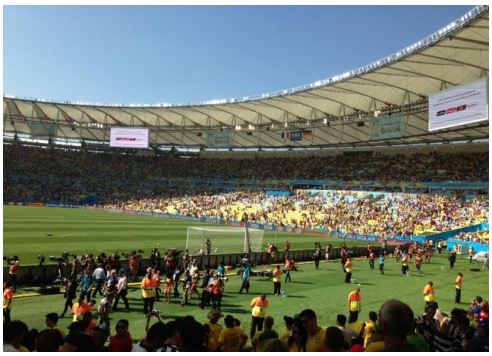
# Major Sporting Events- FIFA 2022 World Cup
# Case Study – Designing in Stadium and Infrastructure Security from the Start

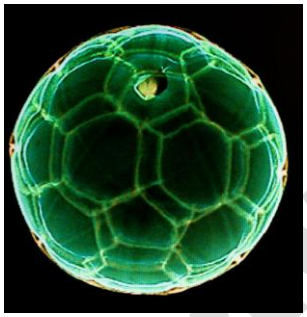
## The Client

The ultimate client was a Supreme Committee responsible for all infrastructure delivery that is required to host a successful FIFA World Cup tournament, in 2022.



## Client Profile

Responsible for building seven new stadiums and precincts and renovating three existing stadiums. As well as providing enhanced and expanded transport infrastructures, as an integrated feature of the World Cup experience. This includes a new metro and light rail system, upgraded airport, new roads, buses and taxis fleets.



A key feature of the projects undertaken is to ensure not only an amazing FIFA World Cup, but also provide a lasting legacy and benefit, to the nation and the region at large. Safety and security is a central pre requisite to the success of the World Cup Tournament. Therefore international security and safety best practices, are embedded at every stage of development.

CYBERRISK.COM
SECURITY - ASSURANCE - FORENSICS - ENABLING

## The Challenge

In relation to the design stages of World Cup Stadium Precincts, lead a comprehensive security risk assessment and provide input and advise, on the cyber and physical security design covering the different operational modes of the stadium.

## Response

Cyberrisk.com worked in close collaboration with stakeholders and the design disciplines such as (architects, engineers, fire safety, stadium operators, crowd modellers) to identify all critical physical and information assets; with respect to their threat and vulnerability profiles. This was an integral process used in the risk assessments, creating a central "living" risk register with treatment and mitigation strategies. Specific security design advice was given under the themes of cyber security and resilience, physical and electronic protective security, counter terrorism protective security and crime prevention through environmental design.

The cyber security assessment was conducted as part of the overall security risk assessment. The cyber risk elements focused on modelling threat and identifying attack surfaces and mitigation strategies, based on the type of exploitation that might occur from a cyber attack. Generally, these were classified into exploits pertaining to spoofing, tampering, repudiation, information disclosure, denial of service (DOS) and elevation of privileges. In terms of physical protection, design and standards advise was given on Hostile vehicle Mitigation (HVM), blast effects and blast protection, ballistics / weapons protection and integrated security. As well as providing functional specifications for CCTV and access control.

## Result

▶ Incorporation of security mitigation strategies and adherence to best practice cyber, physical and operational security standards, throughout the entire design process. Covering preliminary, conceptual and detailed design.

▶ A risk based approach to reducing the vulnerability of critical assets to threats. Thereby ensuring proportionate and cost effective mitigation strategies.

▶ Development of security design reports to inform the various design disciplines as to security requirements, as an integrated risk management model.

▶ Security risks minimised as low as reasonably practicable at the design stage. This will lead to reduced operational or remedial security cost post design.

CYBERRISK.COM

Copyright © 2015 Cyberrisk.com Ltd All rights reserved.
e-mail: hi@cyberrisk.com