MARSH RISK CONSULTING

RISK. DISPUTES. STRATEGY.

Managing the Risks Associated With Catastrophic Events in the Sports Industry

June 2016

MARSH

Why This Topic Was Selected for Today's Webinar
What We Heard From Our Clients

- Disruptive Events (e.g., natural hazards, terrorist threats, riots, pandemics, venue disasters including structural collapses)
- Increasing Customers/Guests/Season Ticket Holder/Vendor Requirements and Expectations
- Concerns from Owners/Executives
- Critical Interdependencies (e.g., reliance on critical resources)
- Questions on the SAFETY Act and How It Works

Today's Discussion and Speakers

- **Pre-event Planning**
  - Our View
  - Emergency Response and Crisis Management
  - Cybersecurity
  - Business Continuity
  - Coverage Reviews and Claims Team

Renata Elias
Consultant
Strategic Risk Consulting Practice
Marsh Risk Consulting

- **Post-event Response**
  - Our View
  - Assessing Impact
  - Deploying Resources
    - Crisis Management, Forensic Accounting, Insurance Recovery

Frank Corrado
FACS Practice Northeast Leader
Marsh Risk Consulting

- **Homeland Security's SAFETY Act – Key Features**
  - What and How
  - Application Process

Ray Biagini
Partner
Covington & Burling LLP

- **Next Steps for the Sports Industry**

Jeff Colburn
US Practice Leader
Marsh Risk Consulting

Catastrophic Events in the Sports Industry

PRE-EVENT PLANNING

The Business Case for Response and Recovery

- In today's environment, you must be able to restore and maintain multiple corporate and operational concerns virtually in unison.
  - Sustaining key functions and processes is extremely difficult if not planned in advance.
- Risks shift and change over time, so you must have a process to account for, and adapt to, the changing landscape.
  - For example, emerging cyber risks necessitate that organizations define cyber broadly (e.g., breach, crime, attack) and that cyber plans also link to overall response plans.
- An integrated and holistic approach is most effective, so you must break down and eliminate silos whenever possible.
  - All specialized plans (e.g., physical security, humanitarian assistance, cybersecurity, emergency response, crisis communication) need to work together when a catastrophe strikes.

Our view: Sports organizations and venues must have a program in place that addresses a broad range of issues and risks, and establishes 'how' the organization will handle potential and actual crises.

Questions to Ask Regarding Your Preparedness

- Does your organization have adequate planning in place to deal with your next emergency, crisis, or business interruption?
- In an emergency, could all of your guests, staff, and vendors evacuate safely and quickly?
- Have you addressed the potential loss of a critical system or business partner that may impact your ticketing, ticket scanning, or point-of-sale operations?
- Is your organization ready to manage the incident or crisis, deal with the surrounding community, continue with operations, and recover from the event?
- When did you last review and test any of your plans?
- Have your key personnel been provided with adequate training to prepare them to respond and manage an emergency, crisis, or business disruption effectively?
- Have security and/or vulnerability assessments been performed?

Safety Act – A Few Key Areas Requiring Advance Work

- Risk Mitigation
  - An overall view of the threats, vulnerabilities for your organization and how you can mitigate and/or minimize their impacts.
  - Clear governance, policies, and protocols related to:
    - Risk identification.
    - Procedures to address various risks when/if they occur.
    - Training and exercising for select personnel.
- Security
  - Mainly targeting physical security systems, monitoring, and protocols for incident response and containment.
  - Security protocols must work in tandem with emergency response, workplace violence, terrorism, and similar plans.
- Cybersecurity
  - An overall approach to addressing cyber events, such as:
    - Cyber privacy or data breach; cyber attack; cyber crime; intellectual property disclosure.
  - Clear linkages need to be made between the IT/tech response and an overall corporate response.

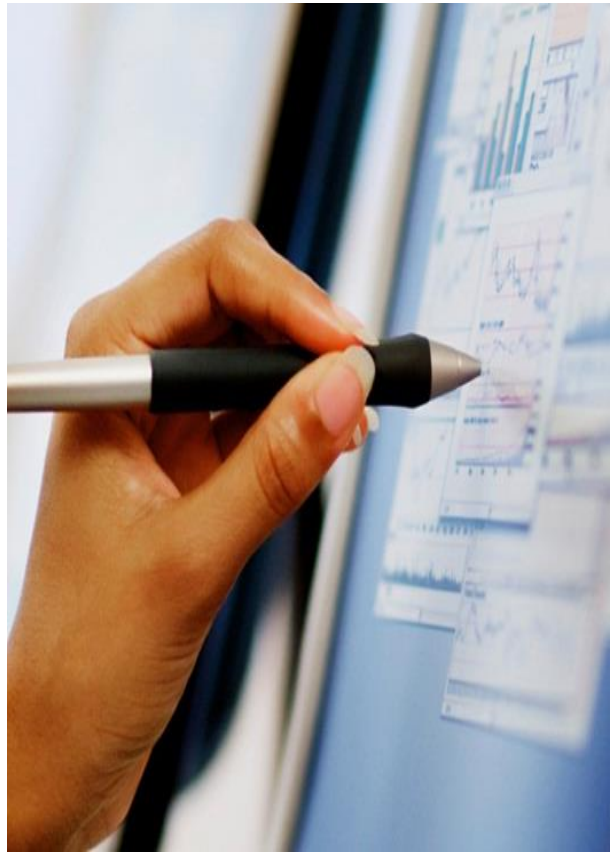
A Cybersecurity Strategy Is Essential

- Cybersecurity practices are essential to sports venue anti-terrorism security. They include, but are not limited to, the following:

1. **Risk assessment process** – prioritize and analyze threats (including cyber attacks) in terms of relative likelihood and consequence.
2. **Information and cybersecurity management** – develop an information security and technology cybersecurity program to protect anti-terrorism technology, systems, and program data with the goal of mitigating exploitation of data or systems which could diminish the effectiveness of, or completely disable, venue security.
3. **Crisis/incident response plan** – prepare plans that provide an incident detection, handling, and response structure, and associated practices, for managing a cybersecurity incident.
4. **External entities** – recognize that external entities may be involved and/or drive your response (e.g., FBI) and plan accordingly in advance.

Business Continuity Management Best Practices

- Identify critical processes.
- Document recovery strategies and recovery activities.
- Document recovery resource requirements, including:
  - People.
  - Systems/applications.
  - Interdependencies.
  - Workaround processes.
- Develop support materials/tools/forms.
- Integrate with crisis management plan/program.



A Closer Look at Some Leading Practices

Our view: If an event impacting your organization occurs, public expectations for how you manage the crisis are significant. Your response may be 'judged' against some of the leading practices highlighted below.

Emergency Response

- Use a common terminology for response actions.
- Establish a flexible, adaptable Incident Command Structure.
- Develop and share discovery, reporting, and alerting procedures.
- Ensure everyone is clear that life safety is the #1 priority.
- Provide consistent training and exercising for general personnel and specialized teams

Workplace Violence

- Establish a policy and threat assessment team to reduce or minimize the risk of workplace violence.
- Establish reporting criteria and processes.
- Identify response processes for minor to major active shooter incidents.
- Collaborate with external stakeholders (e.g., law enforcement, EAP providers, local authorities).
- Conduct training/awareness sessions and drills/exercises.
- Integrate workplace violence plans with other response protocols (e.g., Security, Crisis Communications, Emergency Response).

Crisis Management

- Embed crisis management expectations into all other response and recovery plans – this is the 'executive level' plan that guides decision making at the highest level.
- Consider the full range of risks/crises.
- Create a plan that can be implemented for any type of crisis situation; the process is the same.
- Establish framework, teams, and roles to create response capabilities via briefings and exercises at the senior executive level.
- Establish adequate policies, standards, and governance to guide all risk-related programs.

Pre-Event Planning Approach

OBTAIN LEADERSHIP BUY-IN

ESTABLISH PLANNING TEAM

- Seek cross-functional representation
- Select representatives with decision-making authority within their functional area

CONDUCT PLANNING WORKSHOPS

- Determine response teams and roles
- Identify reporting/escalation requirements
- Capture team activation and meeting process

DEVELOP EMERGENCY RESPONSE AND/OR CRISIS MANAGEMENT PLANS

- Align with other organization plans (e.g., IT/DR, BC)
- Socialize and seek input from first responders (or others you may rely on during an emergency or crisis)

CONDUCT TRAINING/AWARENESS ACTIVITIES

- Identify training for team members and general employees
- Consider quarterly and annual drills/exercises

Prepare for Recovery by Reviewing Insurance Coverages and Establishing a Claims Team

- Review adequacy of policy coverage and limits for property and business interruption (BI).
  - How accurate are your reported values?
  - Discuss loss scenarios, deductibles, and anticipated maximum business interruption loss (AMBIL) within your team and with your insurers.
- Identify your claims team.
  - Your claims team should have business operations expertise.
  - Your claims professionals should have extensive loss experience and insurance knowledge.
    - Broker claim advocates.
    - Forensic accounting/claims preparation experts.

Pre-Event Planning – Fundamentals Recap

- **Align crisis management, response, continuity, security, and recovery capabilities**
- **Consider the whole range of risks facing your organisation**
- **Create response capabilities**
- **Establish adequate policies, standards, and governance**
- **Include preparedness with risk management and mitigation**
- **Involve senior management in the process**

Catastrophic Events in the Sports Industry

POST-EVENT RESPONSE

Post-Event Response Activities

Our view: Post-event response is critical to assessing and managing the financial and other impacts to an organization. This means understanding the scope and magnitude of what happened, how it affected the organization, and the solutions available for recovery. Within the sports industry, some things to consider include:

- First and foremost, prioritize life safety. The sports industry presents risks that could affect large numbers of people and that often invite public scrutiny after an event.
- At the same time, a clear plan as to how to execute a loss recovery and claim preparation process is needed, otherwise the health and wellbeing of the organization could be at risk.
- Prepare in advance to work with law enforcement and civil authorities – including access to sites, the impact of investigations, etc. – so that financial loss recovery can be maximized on a timely basis.
- Physical properties are unique – arenas, stadiums, event venues, etc. – so the loss recovery team needs to have technical understanding, i.e., the involvement of engineers or construction professionals, and understanding of the organization's financial aspects.

Post-Event Response Activities
Immediate Response List

- Contact your broker/claims advocate and notify insurers.
- Set up initial meetings with your claims team (local management, broker/claims advocate, claim preparation professionals, other technical experts) and your insurer's claims team (adjusters and various experts).
- Develop list of damaged assets and assess need to repair/replace.
- Initiate document gathering procedures.
- Prepare preliminary, high-level loss estimates for advance payment purposes.
- Begin developing reconstruction/repair timelines (actual vs. as-was).

Post-Event Response Activities
Initial Inspections and Mitigation Efforts

- Protect property from further damage.
  - Utilize reputable/experienced disaster response service company.
  - Remove water or debris as soon as possible.
  - Secure property.
  - Utilize security services to protect property.
- Perform initial damage assessments.
  - Inspect loss site.
  - Take photographs and/or videos to capture extent of damages.
  - Meet with vendors/contractors.
- Assess need for crisis management and team activation.

Measurement of the Loss
Finding the Right Bucket

- Physical damage:
  - Buildings.
  - Equipment and fixtures.
  - Inventory.
- Time element losses:
  - Business Interruption.
  - Expediting and extra expenses.
- Time element extensions:
  - Extended period of indemnity.
  - Contingent time element/contingent business interruption (CBI).
  - Service interruption.
  - Ingress/egress, possibly civil and military authority.

Property Damage Loss Measurement
Assessment and Repair Estimating

- Assess and document damages to real and business/personal property at all loss locations.
- Determine scope of damage (quantification of property damage) and reach initial agreements with insurer's engineering/property experts regarding scope.
  - Additional technical experts to support scope of damage.
- Establish repair estimate based on historical unit prices (e.g., Means, Marshall Swift, etc.), contractor pricing, and expert reports.
  - As-was repairs vs. betterments.
- Establish repair timelines and schedules.
  - As-was repairs vs. betterments.

Property Damage Loss Measurement
Documentation

- Detailed vendor and contractor invoices:
  - If contractor uses subcontractors, need detailed subcontractor invoices.
- Detailed budgets and proposals:
  - As-was repairs vs. betterments.
  - Hypothetical as-was repair timelines.
- Receipts and expense reports for employee out-of-pocket expenditures.
- General ledger accounting detail and purchase orders.

DOCUMENTATION IS KEY!

THE PURPOSE OF BI COVERAGE

is to put the

POLICYHOLDER BACK IN THE

SAME FINANCIAL POSITION

they would have been in

HAD THE LOSS NOT OCCURRED.

Business Interruption Loss Measurement
Period of Interruption

- Period of indemnity.
  - Gross earnings: based on repair period.
  - Gross profits: based on calendar period (frequently 12 months).
- Theoretical repair period vs. actual repair period.
  - Rebuild “as was” or rebuild including betterments and improvements.
- Extended period of indemnity.

Business Interruption Loss Measurement
Expediting and Extra Expenses

- Expediting expenses.
  - Air freight premium in excess of standard shipping.
  - Overnight shipping/delivery.
  - Overtime/nighttime labor premiums.
  - Identified by specific invoices and labor analyses.
- Extra expenses.
  - Expenses to reduce the loss vs. “pure” extra expenses.
  - Identified by specific invoices.
  - Identified by analyses of income statement expense accounts – excess expenses over and above normal expenses.

Typical 1ST Party Claim Preparation Process

1 Review Policy

Obtain explanations for:

- Limits.
- Payroll cover.
- Increased costs cover.
- Endorsements.
- Basis of settlement.

2 Initial Site Visit

Discuss:

- Bottlenecks.
- Process flows.
- Maintenance.
- Special circumstances.
- Market impact.
- Recovery measures.
- Potential issues.
- Plans.

3 Kick-Off Meeting

Attendees may include:

- Property claims advocate.
- Loss adjuster.
- Insurer's experts.
- Risk manager/client contact(s).

4 Request Initial Information

- Detailed monthly profit and loss statements.
- Chart of accounts.
- Accounting calendars.
- Sales statistics, forecasts, etc.
- All purchase orders, invoices, proof of payment for any PD and EE items.

5 Formulate Initial Estimate

Consider:

- Unusual aspects.
- Loss adjuster concerns/requests.
- Precedents/prior claims.
- Basis of interim claim.
- Internal discussion and agreements.

Ongoing discussions with client, broker, and other key parties.

Continuous claim submissions to secure partial payments and minimize out of pocket expenses.

6 Analysis of Data

Data entry and analysis:

- Reconcile data to explanations.
- Special circumstances.
- Avoided costs.
- Additional costs.
- Formulate initial claim model.

7 Present Initial Findings

- Findings based on data analysis and interviews.
- Discuss reasonableness of results.
- Agree on final approach.
- Request additional info, if needed.

8 Prepare Formal Claim

- Arrange schedules.
- Organize supporting documentation.
- Link supporting documentation to schedules and findings.
- Get final approval/sign off from client on final numbers.

9 Review With Loss Adjuster

- Consider/respond to adjusters comments.
- Calculate effect of adjuster views.
- Review issues, strengths, and weaknesses of our/loss.
- Adjusters methods and conclusions.
- Discuss with client and agree on best course of action.

10 Negotiate Final Outcome

11 Adjuster Report to Insurer

12 Final Settlement Paid

Catastrophic Events in the Sports Industry

HOMELAND SECURITY'S SAFETY ACT – KEY FEATURES

Homeland Security's SAFETY Act
Overview

- As part of the Homeland Security Act of 2002, the US Congress passed the **SAFETY Act** in response to the 9/11 attacks.
- The SAFETY Act is **landmark** legislation, **eliminating** or minimizing 3rd party tort liability, i.e., personal injury, wrongful death, and business interruption damages, for sellers of and those that deploy **anti-terror** technologies (ATT) approved by the Department of Homeland Security (DHS) should suits arise in the US after an act of terrorism.

Homeland Security's SAFETY Act
Certification and Designation

- **CERTIFICATION –** the **highest** form of protection.
  - Presumption that those that deploy ATT are **immediately dismissed** from a suit unless there is **clear and convincing** evidence that the deployer **knowingly and deliberately intended to deceive DHS** in submitting data to DHS during the application process; **no punitives**; suit can be filed only in US federal court; and any liability is **capped** at an agreed upon limit, usually **terror insurance** coverage limits.
- **DESIGNATION –** includes all of the above **except** presumption of immediate dismissal.
  - Designation coverage also available during **developmental, testing, and evaluation** stages of deployed ATT.

Homeland Security's SAFETY Act
Protections and Definition of Act of Terror

- These certification and designation protections also **derivatively protect** seller's/user's subs, vendors, and distributors who contribute to the anti-terror technology.
- Protections will apply **"extraterritorially,"** i.e., where the act of terror occurs **outside the US**, so long as the **"harm," including financial harm**, is to persons, property, or entities in the US.
- Protections can also apply **"retroactively"** to substantially similar deployed ATT.
- The SAFETY Act defines a terrorist attack as **unlawful**, causing **harm** to persons, property, or entities of the US, and using or attempting to use methods designed to cause **mass destruction**.

Homeland Security's SAFETY Act
Types of Anti-Terror Technologies

- The definition of **anti-terror technologies** is **broadly** applied by DHS to cover technologies deployed in **defense against** or **response** or **recovery from** a terrorist attack.
- For sports venues, such ATT includes:
  - **Established** and **documented** security planning procedures and protocols for:
    - Event day vs. non-event day.
    - Emergency evacuation plans.
    - Hiring, vetting, and training of security personnel.
    - Coordination of procedures with governmental entities.

Homeland Security's SAFETY Act
Types of Anti-Terror Technologies

- **Deployed physical security** systems, such as:
  - Perimeter security, including guards and canines.
  - Access intrusion detection systems, including CCTV, magnetrometers, and metal detectors.
  - Command and control centers.
  - Delivery screening and public address systems.
  - Active shooter plans.
- **Deployed cyber security systems**, including recovery, restoration and credentialing technologies.

Homeland Security's SAFETY Act
Length of Protection and Requirements

- Coverage usually awarded for **5 years** from date of decision. However, DHS has also awarded SAFETY Act protections to apply **retroactively** to **past deployments** of "substantially-equivalent" ATT.
- To obtain these tort protections, it is crucial that you demonstrate to DHS the **"proven effectiveness"** and resilience of your ATT, e.g., through **documentation** reflecting your own internal testing/quality control, third-party assessments and evaluations, established vendor selection criteria and processes, etc. DHS wants to see that you **meet** or **exceed** regulatory or industry standards.
- You must carry **terror insurance** as a precondition to obtaining SAFETY Act coverage, in case the presumption of immunity is rebutted. Such terror insurance must respond to **third-party tort** suits.

Homeland Security's SAFETY Act
Process

- To obtain SAFETY Act coverage:
  - Applicants must complete and submit DHS' SAFETY Act Application Kit (**www.safetyact.gov**).
  - The DHS review and approval process takes about **120** days.
  - All application information submitted is kept **confidential.**
  - Application contains three main sections:
    1) **Technical.**
    2) **Insurance.**
    3) **Financial.**

Homeland Security's SAFETY Act
Examples of Certifications

- **Defense and sophisticated products and services contractors** for threat and vulnerability assessment protocols, a secure borders anti-terror program, and an airport baggage handling system.
- A ***Fortune* 50 company** for an innovative application covering the company's internal security practices to protect its high-risk facilities and assets.
- A **sports league** for its stadium security standards and compliance auditing program, which established a baseline level of security at numerous stadiums.
- Three large **professional sports venues** for their security practices and protocols.

Our View on Preparation
Getting the Basics Right

- Pre-event Planning
  - Verify, update, and exercise emergency response and crisis management plans.
  - Complete physical and cybersecurity security reviews.
  - Update business continuity plans for venues and headquarters.
- Post-Event Response
  - Establish response team prior to an event to increase immediate response capability.
- Explore SAFETY Act application process for opportunities to minimize liability from a terrorist act.

QUESTIONS

Marsh Risk Consulting

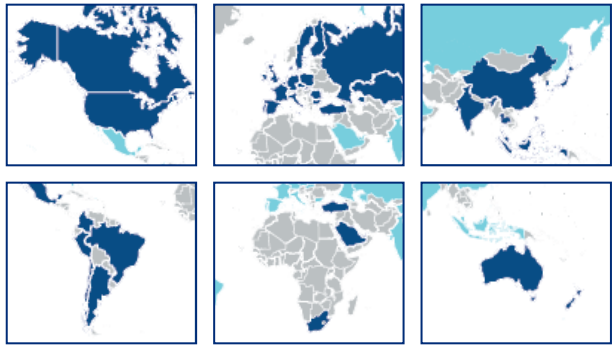
APPENDIX: PRACTICE OVERVIEW

Marsh Risk Consulting

Overview

MRC provides global, customized consulting solutions focused on your business success.

MRC has extensive experience assisting boards, corporate executives, leaders, and risk managers with developing enterprise-wide operational solutions, building resiliency, and achieving their short- and long-term objectives.



VALUE PROPOSITION

Key Capabilities

- Property Risk Consulting.
- Strategic Risk Consulting.
- Cybersecurity Consulting.
- Analytics and Data Management.
- Workforce Strategies.
- Financial Advisory, Claims, and Litigation Support.

Unique Perspective and Global Reach

- More than 800 specialists in over 40 countries.
- Works as one global team with an integrated view of risk.

Deep Technical Expertise

- Experience and expertise across industries.
- Understanding of management drivers and best practices.
- In-depth knowledge of global governance and compliance issues.
- Superior risk modeling and analytics capabilities.

Multidisciplinary Teams

- Cross-practice and cross-geography.
- Alignment with Marsh brokerage and industry practices, and MMC sister companies, to provide a full range of solutions.

Innovative and Customized Approach

- Focused on your needs, objectives, and goals as well as continuous improvement and return on investment.

Award-Winning, Innovative Solutions

- Best Supply Chain Risk Consulting Services Provider, Global Finance (2012, 2014, 2015).
- Risk Manager of the Year, Volker von Widdern, IRMSA (2013).
- Risk Innovator, Risk & Insurance (2010, 2011).
- Innovation Award, Business Insurance (2010, 2011).

Thought Leader on Key Issues, Challenging Conventional Approaches

Our Pre- and Post-Event Risk Management Team

- This team supports:
  - Emergency response planning.
  - Business continuity planning.
  - Crisis management planning.
  - Reputational risk management.
  - Forensic accounting and claims management.
  - Cybersecurity network security assessments.
  - Reconstruction services.
- Our core team consists of senior consultants with experience supporting a variety of organizations and facility types in the sports industry. This includes:
  - Leagues.
  - Teams.
  - Venues.
  - Stadiums.
  - Arenas.

Contact Us

Scot Ferrell
US West Zone Growth Leader
Marsh Risk Consulting
+1 415 743 8646
scot.ferrell@marsh.com

Ray Biagini
Partner
Covington & Burling LLP
+ 1 202 662 5120
rbiagini@cov.com

Thank You

MARSH RISK CONSULTING