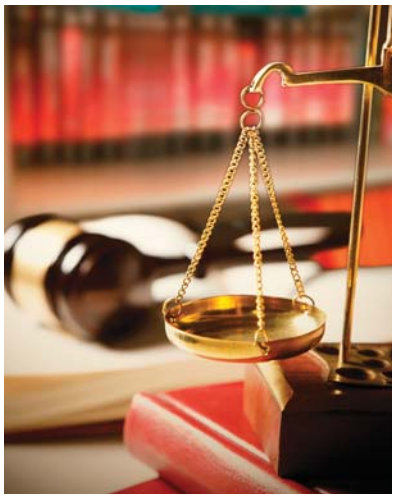
MARSH INSIGHTS:

THE HILLSBOROUGH DISASTER: LESSONS IN LEGAL COSTS AND LIABILITY

The Hillsborough disaster emerged as one of the worst disasters in sporting history, and remains the most devastating in UK football history. In 1989, an FA cup semi-final game between Liverpool and Nottingham Forest at Sheffield Wednesday's Hillsborough ground resulted in overcrowding in the Liverpool fans' allocated area. 96 people died and hundreds more were injured after being crushed against the standing pens within the stadium.

Court proceedings regarding the liability of the event concluded in April 2016, with liability attributed to lack of crowd-control measures by police. Government figures revealed in ***The Guardian***[1] indicated that the Home Office spent GBP63.6 million covering the legal costs of the families of the 96 victims of the Hillsborough disaster. The bill[2] includes the cost of solicitors, experts, counsel, and disbursements between 31 December 2012 and 30 June 2016.

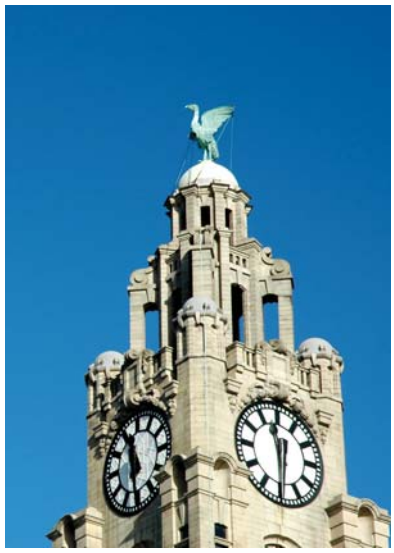


However, it is unclear how much of liability insurance levels were taken up by legal costs, possibly meaning much of the liability was not covered under insurance. When considering major incidents, it is important to understand the limits of liability in your insurance policy and how legal costs impact the insured amount. You should know whether your policy includes legal costs within this limit, as often the entire limit of liability can be taken up by ongoing legal costs before liability amounts are decided.

Given the number of parties involved in a major sporting event, if something goes wrong' liability costs can stem from a number of sources including:

- Venue owners.
- Sporting body (for example, the national governing body of the sport).
- Police/security organisations.
- Event organiser.

One consideration for parties involved in major events today is that insurance liability limits of indemnity may need to be much higher than they were when the Hillsborough disaster took place due to the increasing value of professional sportspersons, larger capacities of venues, and the legal costs associated with litigation.



While considerable improvements in crowd safety have been made since 1989, it is still important that all parties are mindful of the possible risks involved in a sporting event with a large crowd. Injuries and crushing due to crowds is still a key risk to take into consideration, and appropriate measures should be put in place to ensure the safety of individuals.

1 Perraudin, Frances. "Hillsborough families' taxpayer-funded legal fees exceed £63m", ***The Guardian***, 3 November 2016, available at https://www.theguardian.com/football/2016/nov/03/hillsborough-families-legal-fees-costs-home-office, accessed 15 November 2016.

2 "Bereaved Hillsborough families: legal representation costs", available at https://www.gov.uk/government/publications/bereaved-hillsborough-families-legal-representation-costs, accessed 15 November 2016.

WORKFORCE SECURITY: PROTECTING YOUR EMPLOYEES

The global nature of sport often requires an organisation's workforce to be deployed all around the world – often in territories that present an increased risk exposure in respect of security, political unrest, and/or natural perils.

The England men's cricket team, for example, recently toured Bangladesh to play test cricket. The high-level security operation surrounding the team was a resounding success, despite the event taking place in a country that has experienced a string of terrorist incidents in recent years.

As a result, the Government of Bangladesh and Bangladesh Cricket Board (BCB) have dramatically enhanced the country's reputation for security and protected its near-term future as host to international cricket events. Had a security incident occurred, things could have been very different.

Whether you're a governing body, federation, association, union, or club, protecting the welfare of your employees is of paramount importance. Given the media scrutiny professional sportspeople receive, there is an intensified threat which can be managed by having a well-executed risk transfer strategy in place.

Terrorist and other criminal attacks can threaten your people, operations, and assets. Many organisations look to insurance — mainly property, terrorism, and political violence coverage — to help manage the financial impact of these risks, which can include property damage and business interruption (BI).

Political and natural disaster evacuation insurance can be designed to protect you against the costs incurred in evacuating the various employees you have chosen to insure, their partners and dependants, and, if applicable, any local national staff, as a result of a political or natural disaster.

Such policies typically pay for:

- The additional costs incurred in providing increased security at your current location, or for the costs of relocating at a site chosen by our crisis management company, for up to 14 days after an insured event has occurred.

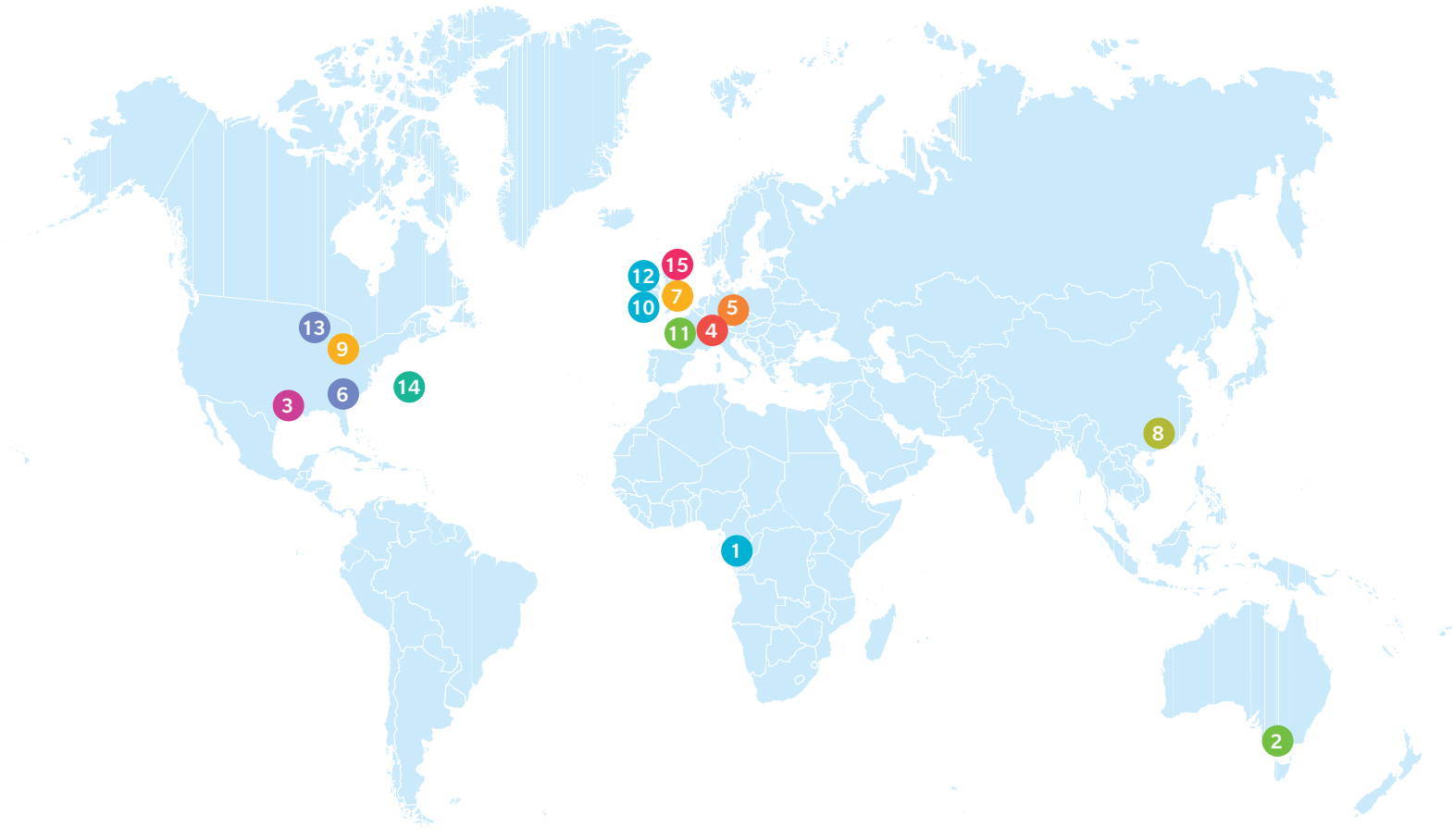
- The costs of transporting and accommodating additional personnel with the relevant skills to facilitate the evacuation and the breakdown of equipment following an insured event. Coverage is purchased in addition to a standard personal accident and travel policy. No matter which country you are domiciled in, cover can be specifically tailored to your requirements.

Marsh's PanOptimum insurance cover product is an all-in-one risk solution for workforces working abroad and satisfies the need for international organisations to have effective risk management programmes in place to protect employees during emergencies. It enables organisations to purchase an all-in-one combination of cover for the most prevalent risks, including political and natural disaster evacuation, group personal accident and medical, and kidnap and ransom.

For more information, speak to your local Marsh representative.

GLOBAL SPORTS EVENTS 2017

1	14 January-5 February	Football	African Cup of Nations	Gabon
2	16-29 January	Tennis	Australian Open	Melbourne, Australia
3	5 February	American Football	Super Bowl	Texas, US
4	6-19 February	Skiing	World Alpine Ski Championships	St. Moritz, Switzerland
5	14-24 March	Multi-sports	Special Olympics World Winter Games	Graz and Schladming, Austria
6	3-9 April	Golf	Masters	Georgia, US
7	8 April	Horse Racing	Grand National	Liverpool, UK
8	12-14 April	Cycling	World Track Championships	Hong Kong
9	6 May	Horse Racing	Kentucky Derby	Kentucky, US
10	27 May	Football	FA Cup Final	London, UK
11	28 May-11 June	Tennis	French Open	Paris, France
12	3 June	Football	UEFA Champions League final	Cardiff, UK
13	15-18 June	Golf	US Open	Wisconsin, US
14	17-27 June	Sailing	America's Cup	Bermuda
15	26 June-23 July	Cricket	Women's World Cup	UK



WHAT TO DO WHEN DIGITALISATION GOES WRONG

Cyber risks have recently come into focus for sporting organisations following hacks impacting the industry. Given the personal and medical data held by sporting agencies, how prepared are you for a worst-case scenario?

For years, conventional wisdom has dictated that organisations focus on preventing the most common types of cyber attacks, rather than preparing for that one all-encompassing disaster that might never occur. But in reality, it is no longer possible to make such a trade-off. Full-blown cyber crises – some of them life-threatening – are becoming more common.

Increasing digitalisation and interconnectedness are exposing organisations more frequently to more sophisticated kinds of cyber threats. Planning for worst-case scenarios is no longer optional.

Consider that just last year 500 million personal records were stolen or lost. Ransomware attacks grew by 35% and spear-phishing incidents by 55%. These types of attacks are no longer just harming desktop computing. They are starting to cause the malfunctioning of critical medical equipment, emergency services, and fundamental communications. Few organisations' cyber defences are keeping pace.

We estimate that only a third of companies are sufficiently prepared to prevent a worst-case attack. Based on a recent survey by Marsh, a quarter of companies do not even treat cyber risks as significant corporate risks. Nearly 80% do not assess their customers and suppliers for cyber risk.

As companies roll out more digital innovations, they need to adopt more flexible and ubiquitous cyber defence measures to meet the more extreme threats they now face. Failing to do so risks unanticipated costs, operational shutdowns, reputational damage, and legal consequences. For example, in response to growing ransomware and spear-phishing attacks, many leading organisations are drawing up back-up plans to operate offline in the event that their operations are crippled. Some are going even further and making operating offline their preferred approach. In response to hacktivists crippling the government's websites through a series of cyber attacks in 2013, Singapore is cutting off access to the internet for nearly all government computers. Healthcare providers and hospitals in the US and Germany are taking critical systems partially offline where connectedness is not required, and are prepared to go back to pen and paper in case an incident impairs their digital operations.

NEW DATA STRATEGIES

Some organisations are changing the way they use and store data. Classic forms of data and legacy information technology systems are not flexible or smart enough to keep up with rapidly shifting needs to protect records. To respond to cyber threats more rapidly, some companies are radically simplifying their business setups and technical systems. By doing so, companies limit the places where a hacker can enter and hide. Splitting data up and storing the pieces in different systems also reduces the amount of sensitive data that is vulnerable at any one time.

Other companies are replicating their core information technology systems so clients can receive basic services even if their own systems entirely collapse.

CONCLUSION

The cyber threats previously considered to be unthinkable are now daily news. To avoid becoming another headline, organisations must prepare for the worst – including the unthinkable.

This article has been adapted from one that originally appeared in the MMC Cyber Handbook 2016.

CYBER AND CRIME INSURANCE OVERVIEW

Your organisation can purchase cover for business interruption under a commercial combined policy for physical damage, such as fire. However, a commercial combined policy does not provide cover for intangible risks such as a hacker preventing your IT software from operating. This risk would fall under a cyber insurance policy. The main cyber insurance coverages are as follows:

COVER	WHAT DOES IT DO?	APPLICATION/CLAIMS SCENARIOS	BENCHMARK INFORMATION
Privacy liability Multimedia liability Network liability	Protection against third party liability claims and regulatory actions arising from the unauthorised disclosure of personal information. It will also pay regulatory fines (where insurable at law) arising from the same event. Protection against third party liability arising due to breaches of network security, including negligent transmission of computer virus or denial of a third party's authorised access to computer systems. Protection against third party liability arising from defamation, infringement of their intellectual property rights, invasion of privacy resulting from the content of your website, blogs, or other online material.	IT system gets hacked and hacker manages to obtain credit card information held by your organisation. Your organisation is deemed to be the "data controller". Customers demand damages from you for breach of privacy. A database of names gets breached. Customers demand damages from you for breach of privacy. Following a breach of payment card industry (PCI) data security standards, your business is investigated and subsequently fined. Costs of complying with the investigation and PCI fines are insured by this section as PCI fines are insurable under current UK legislation. Information Commissioner's Office (ICO) investigates you for cyber breach. Defence costs are covered by cyber policy. Currently UK legislation precludes any ICO fine from being Insured.	Most organisations that purchase cyber include this module.
Privacy breach costs	Protection for the costs incurred by your organisation in responding to an incident involving the unauthorised disclosure of personal information. The costs insured include, IT investigation costs, legal advisory costs, data subject notification costs, data subject credit monitoring costs, and public relations costs.	Your IT system or database gets hacked and the hackers manage to obtain sensitive data/credit card information/names and addresses. Your organisation decides to notify all customers that their details may have been compromised. Notification costs, credit monitoring etc. are covered by this module.	Many businesses that purchase cyber cover include this module. These are for your own costs in notifying customers, credit monitoring, and public relations costs etc.
Data asset protection	Protection for the cost of reconstituting data that has been deleted, stolen, or corrupted due to a breach of network security and certain other specified events.	Your organisation's website is hacked and a virus is inserted. After a period of time, the hacker activates the virus and data is wiped/encrypted. The virus is also in your back-up systems and you incur costs to re-constitute data.	Purchased by some organisations who buy cyber cover.
Cyber extortion	Protection for the cost of engaging an expert in handling certain defined cyber extortion threats and for the cost of a ransom to prevent the threat being carried out.	You receive a demand for a monetary amount otherwise a third party will take down your system.	Majority of businesses which purchase cyber include this module.
Cyber network interruption	Protection for loss of net profit and increased costs of working arising from the unavailability of information technology due to breaches of network security and other specified events.	Your IT systems is: • Hacked and is not restored to full operation for 48 hours. • Corrupted by employee error and is not restored to full operation for 48 hours. • Not restored to full operation for 48 hours after an outsourced service provider encounters a problem.	Less common purchase due to the individual perceived exposure to risk. Organisations with cloud services do tend to purchase cover.

Most cyber policies do not currently extend to include crime. A specific crime policy will usually be required for the following scenarios.

COVER	WHAT DOES IT DO?	APPLICATION/CLAIMS SCENARIOS
Crime	Protection against unauthorised electronic funds transfer, theft of money or financial assets by electronic means, or fraudulent manipulation of electronic documentation. Telephone hacking.	Theft of money /digital assets by fraudulent third party such as phishing, fake CEO/president scams. Hacker accesses your telephone system and uses it to generate unauthorised calls passing the bill to your account.

CYBER INSURANCE SERVICE OFFERING

Many cyber insurance policies provide immediate response services in the event of a breach. If you are placed with one of the insurers offering this service, you will have immediate access on a 24-hour/365-day basis to specialist support in respect of an actual or suspected breach of personal information, security failure, or system failure as follows:

i. A response adviser for the provision of the legal advice and support.

ii. An IT specialist in providing first response IT services to:

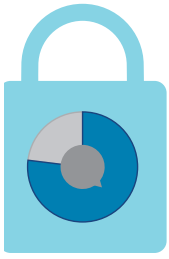
- Establish whether security failure or system failure has occurred, how it occurred, and whether it is still occurring.
- Identify whether a security failure or system failure has resulted in a breach of personal information or a breach of corporate information.
- Establish the extent of any personal information or corporate information that may have been compromised.
- Contain the security failure or system failure, including a denial of service attack.

iii. A crisis consultant to provide public relations or crisis communications services.

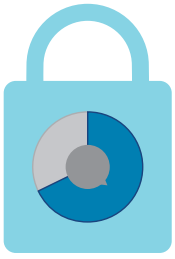
iv. A cyber extortion adviser to negotiate with the instigator of an extortion demand and, if necessary, pay the ransom demand.

Depending on the insurer chosen, the monetary excess does not apply to this response service and no additional charge is made for its use.

THE STATE OF CYBER RISK MANAGEMENT AT A GLANCE

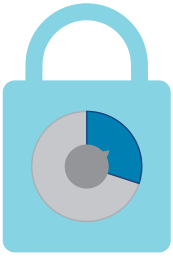


77%
of corporations do not assess their suppliers or customers for cyber risk.

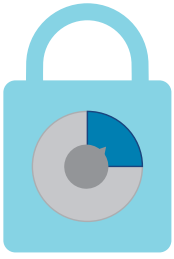


68%
of corporations have not estimated the financial impact of a cyber attack.

43%
of corporations have not yet identified one or more cyber scenarios that could affect them.



30%
of corporations have less than a basic understanding of their cyber risk exposure.



25%
of corporations do not include cyber risks in their corporate risk registers.

Source: *European 2015 Cyber Risk Survey Report*, Marsh, Global Risks 2015

NEW UK SPORTS GOVERNANCE CODE

Following the publication of the Charter for Sports Governance in the United Kingdom in May 2016, UK organisations seeking public funding for sport and physical activity must now comply with a new "Sports Governance Code".

This new Code, announced last month, sets out the levels of transparency, accountability, and financial integrity that will be required from those who ask for Government and National Lottery funding from April 2017.

The Code has three tiers of compliance and will apply to any organisation seeking funding from Sport England or UK Sport, regardless of size and sector, including national governing bodies of sport, clubs, charities, and local authorities.

It works in proportion to investment amounts, requiring the highest standards of good governance from organisations requesting the largest public investments.

- Tier 3 (top level): This level requires mandatory compliance with all code requirements. This typically applies to organisations with GBP1 million or more in funding over a period of years.
- Tier 2: All Tier 1 requirements, plus some bespoke requirements of Tier 3. This typically applies to large, one-off investments, exceeding GBP500,000.
- Tier 1: A minimum level of compliance with requirements. This typically applies to one-off investments of under GBP250,000.

The Code also lays out some key elements of what would constitute good governance from organisations. Some key elements include:

- Increased promotion of skills and diversity in decision making, with a target of at least 30% gender diversity on boards.
- Greater transparency, such as publishing more information on the structure, strategy, and financial position of the organisation.
- Constitutional arrangements that give boards the primary role in decision making.

All organisations in receipt of public funding must complete and publish an annual governance statement that sets out how they have met the requirements of the new Code.

KEY AREAS OF THE CODE FOR SPORTS ORGANISATIONS

STRUCTURE

The Code outlines several structural requirements, including that:

- The board must be the primary decision maker – not committees or councils.
- The board structure should include 12 people in total, with an appropriate skills matrix, term limits, and a four-year gap before re-appointment. A quarter of it should be made up of independent directors, with senior independent director appointments.
- Councils should have defined roles, specified term limits, and be open and transparent.
- Committees for audit and, in some cases, nominations should be established.

INTEGRITY

Those who lead the organisations must work to the highest standards of integrity, and those holding senior positions of office (for example, board members, trustees, or chief executives) will sign a declaration which sets out:

- A commitment to the organisation's purpose, aims, and objectives.
- That they are of "good character", have the necessary skills and experiences for their role, and their professional conduct while in office will be of the highest standard.

Organisations must also demonstrate that they have adequate education programmes and prevention measures in place to protect against sport manipulation.

PEOPLE

The Code also sets out key principles in promoting diversity, independence, skills, experience, and knowledge.

- Organisations should aim to have at least 30% gender diversity on the board.
- Public commitment to achieve broader diversity.
- Skill-based appointments.
- Public disclosure of information.
- Remuneration disclosures.

Sport England and UK Sport will develop a single assessment procedure in terms of compliance with the Code and are looking at developing and publishing benchmarked data.

FOSTERING DIALOGUE: THE MARSH SPORTS AND EVENTS COMMUNITY

Within the global Marsh Sports and Events Practice we serve a multitude of clients around the world. In order to learn about best practice and find out more about our activities and customised risk and insurance solutions, join our Marsh Sports Forum on LinkedIn.

Join our LinkedIn group **here.**

CONTACTS

For further information, please contact:

RICHARD TOLLEY
EMEA Sports and Events Leader
+44 (0)121 623 1389
+44 (0)7774 985 580
richard.n.tolley@marsh.com

LENNOX BATTEN
Managing Director, Personal Accident, Contingency, and Events Practice
+44 (0)20 7357 3054
+44 (0)7775 674 534
lennox.batten@marsh.com

WARREN HARPER
Global Sports and Events Practice Leader
+1 404 995 3556
+1 404 200 7878
warren.h.harper@marsh.com

GRAPHICS NO. 16-1185